ヒューマンファクタによる情報リスクを技術で低減するオフィスセキュリティ

甲斐　賢

謝辞

本論文は，筆者が平成 22 年 10 月に京都大学大学院 情報学研究科 社会情報学専攻の博士後期課程に編入し，京都大学教授 喜多 一 先生，NPO 法人情報セキュリティ研究所 上原 哲太郎 先生の懇切丁寧なご指導とご助言をもとにまとめた研究成果です．ここに謹んで厚く御礼申し上げます．

研究を進める上でアドバイザーとして御指導いただきました，京都大学 吉川 正俊 教授，東京工科大学 手塚 悟 教授に深く感謝致します．

論文審査を通じまして，御指導いただきました，京都大学 岡部 寿男 教授，京都大学 山本 章博 教授に深く感謝致します．

快く社会人博士後期課程への編入を認めていただきました，独立行政法人 産業技術総合研究所 セキュアシステム研究部門 寶木 和夫 副研究部門長および株式会社 日立製作所 情報・通信システム社 スマート情報システム統括本部 藤城 孝宏 部長に心より深く感謝致します．

本研究を進めていくにあたり，日頃からご意見をくださった，株式会社 日立製作所 横浜研究所 エンタープライズシステム研究部 SE5 研究ユニットの 鍛 忠司 主任研究員をはじめとするユニットメンバー諸氏に感謝致します．

最後に，博士論文を書く長い間，生活面で支えてくれた妻 順子 に感謝します．

平成 24 年 8 月　甲斐　賢

概要

近年，企業や組織にとって，情報セキュリティ対策の実施は必須事項である．情報セキュリティ対策で論じられる Weakest Link（最も弱い箇所）は，これまで IT の進歩と共に変化してきた．1960-70 年代はメインフレームにおける OS セキュリティコントロールの欠陥，1980 年代は PC へのフロッピーディスク経由でのウイルス感染，1990 年代はインターネット境界外からの不正侵入と言われてきた．特に 2000 年代以降はワークステーション（端末側）やヒューマンファクタの問題が大きいと言われる．セキュリティ対策にかかる全体コスト TCO は，主に経営者や責任者が担う Plan フェーズの上流工程よりも，主に従業員が担う Do フェーズおよび経営者・責任者から従業員までが関与するインシデント対応フェーズといった下流工程の方が圧倒的に大きくなる．そのためヒューマンファクタの問題が大きいことは認識されていても，対策にはなかなか踏み込めなかった分野である．

本研究では，上記のヒューマンファクタの問題に対して，解決のための新たな 3 種類のオフィスセキュリティ技術を開発した．1 つ目の技術は，情報漏えいリスク，特に紙文書からの漏えいリスクに対して，従業員の過失による印刷ミスを防ぐための，重要印刷検出技術である．重要印刷検出技術は，印刷文書のテキストを抽出するのに，OCR を使わずに，プリンタドライバ内での文字コード処理を直接フッキングして行う．従来の OCR を使ったテキスト抽出に比べて，正確さと高速性の点で有用である．2 つ目の技術は，同じく紙文書からの漏えいリスクに対して，従業員の故意による印刷を抑止するための，印刷監視・調査技術である．印刷監視・調査技術は，印刷文書のテキストとサムネイル画像を取得することで印刷ログの容量を小さくし，全文検索サーバにより常時インデックス化を行う．もし漏えいインシデントが発覚した場合にはハードディスクを解析する従来のデジタルフォレンジック技術に比べて，1 週間以内に一次報告を行うための調査人員を削減できる点で有用である．3 つ目の技術は，未知ウイルス感染リスクに対して，従業員の端末側に残る重要ファイルの漏えいや改ざんを防止するための，ウイルス封じ込め技術である．ウイルス封じ込め技術は，従来のブラックリスト型とは異なるホワイトリスト型を採用し，さらに端末一台一台に適したホワイトリスト型のアクセス制御ポリシーを，知識や訓練の少ない従業員でも容易に設定できる点で有用である．

以上，研究開発してきたオフィスセキュリティ技術は，セキュリティ対策にかかる TCO をとくに下流工程において削減する効果を持つことが期待される．つまり上記オフィスセキュリティ技術は，従業員がセキュリティを意識しすぎるあまりに業務がうまく回らないという「セキュリティによる窒息」を解消することに貢献する．

Abstract

Recently an enterprise or an organization must perform information security countermeasures. The weakest link, discussed in information security, has been changed according with IT progress. In 1960s to 1970s, the weakest link was a flaw of OS security controls. In 1980s, it was a virus infection via a floppy disk. In 1990s, it was an invasion from a firewall's border via the internet. In 2000s, the weakest link was a problem of a workstation and a human factor. Total Cost Ownership of security countermeasures, mainly composed of both an upper "plan" process by a business manager or a division manager and a lower "do" process by employees or "incident response" process by manager and employees, becomes bigger and bigger in a lower process than in an upper process. Therefore, the human factor has been a difficult to resist even if it was known as a big problem.

This research focused the above human factor problem and developed three kinds of office security technologies to resolve the problem. First technology is a detection of important print-out to resist information leakage from a paper-medium, which prevents employees from print-out miss or error. The detection technology identifies a print-out content not by using OCR (Optical Character Recognition) but by using device driver hooking of character code processing to extract full-text. This technology improves an accuracy and speed compared to a conventional OCR. Second technology is a print-out monitoring and investigating to resist information leakage via a paper-medium, which restrain employees from print-out with an evil purpose. This monitoring and investigating technology reduces a log size by acquiring both full-text and a thumbnail image of a print-out content, and makes search indexes by using a full-text search server. If information leakage happens, the technology reduces a number of investigators who are responsible to something to report within a week, compared to conventional Digital Forensics that analyzes a hard disk of PC directly. Third technology is a virus containment to resist an unknown virus, which prevents important files left on clients from leakage or falsification. The containment technology adopts a white-list type approach different from a conventional black-list approach, and

makes easier to configure a white-list policy suitable for every client PCs without deep knowledge or training of employees.

To sum up, these office security technologies are expected to reduce security TCO especially for lower "do" or "incident response" processes. In other words, the technologies contribute to get rid of "suffocation by security" status, which means that too excessive employee's consciousness of security interferes in usual works.

目 次

図 目 次

表 目 次

第1章　序論

1.1　研究の背景

近年，企業あるいは組織にとって，情報セキュリティ対策の実施は必須事項である．特に情報セキュリティ対策は事業所つまりオフィスの単位で実施することが多く，事業所単位で実施するセキュリティ対策の代表例であるプライバシーマーク [1] や ISMS（Information Security Management System）[2] などは，図 1.1 に示すように，それぞれ 12,000 以上，3,700 以上の事業所が取得している．これらのセキュリティ認定・認証を取得するためには，図 1.2 に示すように，入退室管理などの (1) 人的リスク対策，書類・ロッカーなどの (2) 物的対策，クライアント PC やサーバなどの (3) 情報リスク対策など，幅広いセキュリティ対策が必要となる [3, 10].

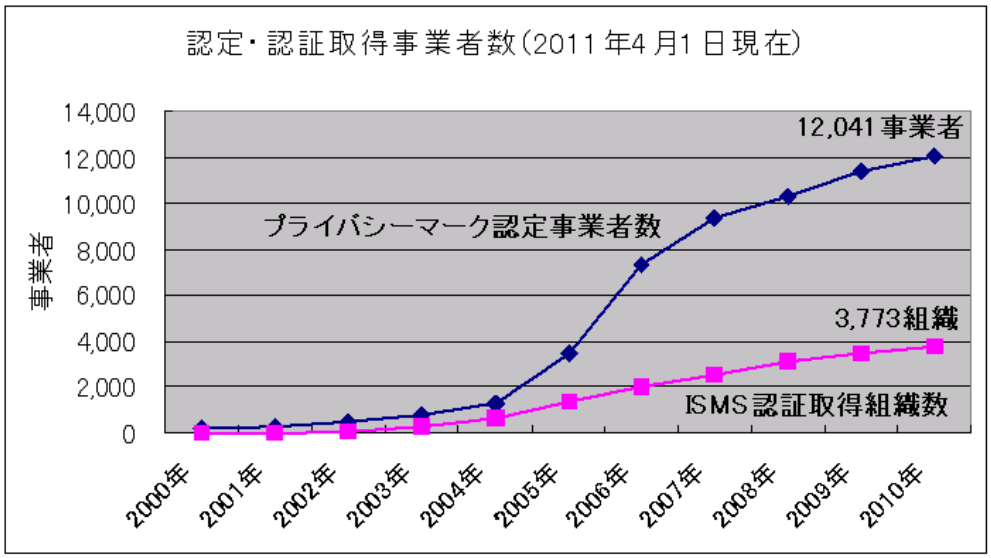

図 1.1: プライバシーマーク認定事業者数と ISMS 認証取得組織数（出典 [1, 2] のデータをもとに作成）

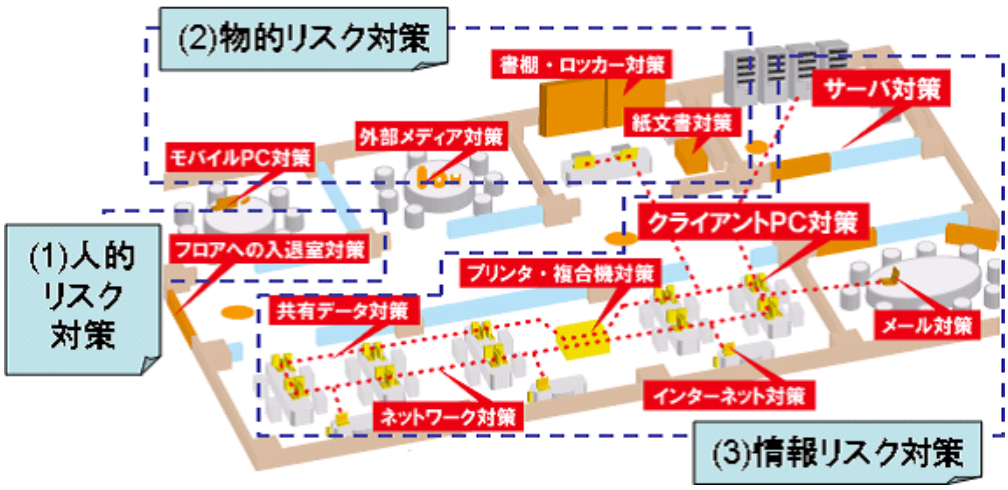

図 1.2: 事業所で必要となるセキュリティ対策例（出典 [3] の図に加筆）

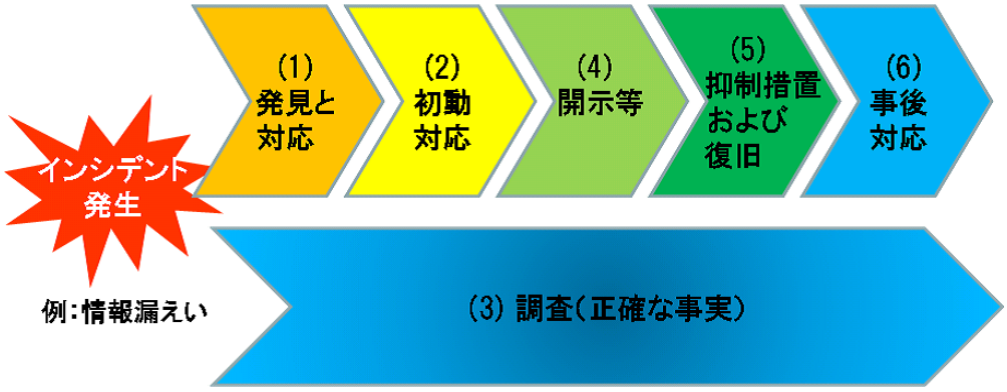

図 1.3: 情報漏えい発生後のインシデント・レスポンスのステップ（出典 [4] の図に加筆）

しかしいくらセキュリティ対策を実施してもセキュリティインシデント（情報漏えいなど）の発生がゼロになるわけではない．もしセキュリティインシデントが発生すると，図 1.3 に示すように，(1) 発見と対応にはじまり (4) マスメディアなどへの開示を行いつつ (6) 通常のビジネスに復帰するまでに早くて数週間，遅くて数年に及ぶ (3) 調査を強いられることになる [4].

このようにセキュリティ対策はコスト，つまり収入を増やすことには関係しない出費と取られやすいが，一方でセキュリティ対策への投資をゼロにすることはいたずらにリスクを増やしインシデントの発生を許すことにもなる．実際，セキュリ

ティ対策に関する投資対効果（ROSI, Return on Security Investment）は，式 1.1 で表現される [11]．つまり，さらされるリスクの大きさ（Risk Exposure）とリスク軽減率（% Risk Mitigated）の掛け算と，ソリューション費用（Solution Cost）との差によって効果を測定する．

$$ROSI = \frac{(RiskExposure \times \%RiskMitigated) - SolutionCost}{SolutionCost} \tag{1.1}$$

具体的にはウイルス対策を例にとると，

- 1 回のウイルス感染により，生産性が$25,000 ほど低下する
- ウイルス対策ソリューションの適用前には，年に 4 回ほど感染していた
- ウイルス対策ソリューションコストが$25,000 である
- ウイルス対策ソリューションを適用することで，感染回数が年に 1 回に減った

とした場合には，Risk Exposure は $\$25,000 \times 4 = \$100,000$，%Risk Mitigated は $\frac{(4-1)}{4} = 0.75$，Solution Cost は$25,000 となる．この場合の ROSI は，式 1.2 に示すように計算される．

$$ROSI = \frac{(\$100,000 \times 0.75) - \$25,000}{\$25,000} = 200\% \tag{1.2}$$

このような ROSI の計算式から見ても，**セキュリティ対策は必然的に，投資とリスクのトレードオフを抱える**ものと言える．

投資とリスクのトレードオフは事業所の構成要員に大きな影響を及ぼすことが想定される．警察庁が毎年公表している不正アクセス行為対策等の実態調査 [12] にある「投資に関する考え方」の分析結果を整理すると，大きく「経営者・責任者」「IT スタッフ」「上長・マネージャ」「従業員」に分けて，以下に示すようにそれぞれの立場で異なるジレンマを抱えると整理できる．

経営者・責任者
: 情報リスクは経営にも影響する．一方，収入にならないセキュリティ投資は減らしたい

IT スタッフ
: セキュリティ製品を導入すれば情報リスクは減る．一方，製品の使い方や運用に関するヘルプデスクに関するコストがかかる．例えばパスワードを忘れた場合のリセットなど．

上長・マネージャ
: 自身の管理部署からはセキュリティ事故を起こしたくない．事細かに管理すれば防げるかもしれないが，多くの従業員を管理するのは手が回らない．

従業員
: セキュリティ対策を行うことも仕事の一つである．一方，セキュリティ対策ばかりでは収入にならないため，本来の業務を圧迫されたくない．

1.2 研究の範囲

投資とリスクのトレードオフの問題を体系化するため，本論文での研究範囲を述べる．

1.2.1 Weakest Link

鎖の強さはもっとも弱い輪と同じだけの強さであると言われる．つまり，他の輪がどれだけ強くても，鎖の全体としての強さはもっとも弱い輪で決まる．企業や組織におけるセキュリティ対策も，鎖と同様，もっとも弱い輪（Weakest Link）で決まると言える．セキュリティの Weakest Link は，表 1.1 に示すように，IT の進歩に応じて変化してきた [8].

表 1.1: セキュリティの Weakest Link（出典 [8] をもとに作成）

年代	IT の進歩・普及	Weakest Link
1960-70 年代	メインフレーム	OS セキュリティコントロールの欠陥
1980 年代	PC	フロッピーディスク経由で感染するウイルス
1990 年代	インターネット	ネットワーク境界の外からの不正侵入
2000 年代	Web ブラウザ 電子メール	OS やソフトウェアのセキュリティホール ヒューマンファクタ

1960-70 年代はメインフレームの時代であった．メインフレームは物理的に隔離されることが多く，そのため出来心の攻撃者であっても強い意思をもつ攻撃者であっても，アクセス機会が少ないこと自体が障壁であった．メインフレームの Weakest Link は OS（オペレーティングシステム）セキュリティコントロールの欠陥であり，OS セキュリティの研究 [13] が進歩した．

1980年代はPC（パーソナルコンピュータ）が，家庭利用やレジャー利用として普及し，そのため新しいセキュリティ問題，つまりコンピュータウイルスの問題が発生した．当時フロッピーディスクでデータをやり取りする機会が多く，フロッピーディスク経由で感染するウイルスが問題となった．ウイルスとは，第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり，自己伝染機能，潜伏機能，発病機能のうち一つ以上を有するものである [14].

1990年代はインターネットの普及と共にネットワークシステム化が進んだ．ファイアウォールは外部ネットワークと内部ネットワークとを分ける標準的なセキュリティ対策として導入が進んだ．しかし，外部からのアクセス者が仲間なのか敵なのかを判定することは困難であり，ネットワーク境界の外からの不正侵入の問題が大きくなった.

2000年代は企業や組織において一人一台のワークステーションが割り当てられ，Webブラウザや電子メールソフトウェアといったPeer-to-Peerなネットワーク利用が普及した．しかし，セキュリティ管理者は個々のワークステーションまで管理が行き届きにくく，そのため，ワークステーションで利用するOSやソフトウェアのセキュリティホールが問題となった.

さらに企業や組織の情報資産やIT資産は，最終的には人間が扱うものであるため，**ヒューマンファクタの問題**も大きくなってきた [15–18]．ITスタッフであれば過剰な権限を与えられた場合に，本来定められた権限を超えた操作をおこなうと言った内部犯行につながりかねない．従業員であれば十分や教育や訓練が行われるとは限らず，過失の問題も大きい.

本論文では，2000年代以降に顕在化してきた，ワークステーションやヒューマンファクタの問題を研究対象とする.

1.2.2 セキュリティTCO

企業や組織におけるセキュリティ対策には，多くのコスト（時間・人員）がかかる．セキュリティ対策にかかるコストは，情報システムへの投資全体に対する割合で論じられることが多く，一般には3-7%程度と言われている [19–21]．セキュリティ対策にかかるコストの内訳を分析した文献 [22] では，対策にかかるコストを，インシデント発生を防止するためのコストとインシデント発生後のコストに分けている．こうした考え方に基づくと，セキュリティの総コストつまりセキュリティTCO（Total Cost of Ownership）は，組織の構成要員の各立場の点で，図1.4に示すように整理できる.

経営者・責任者は，セキュリティ対策のPlanフェーズ，つまり戦略立案や予算

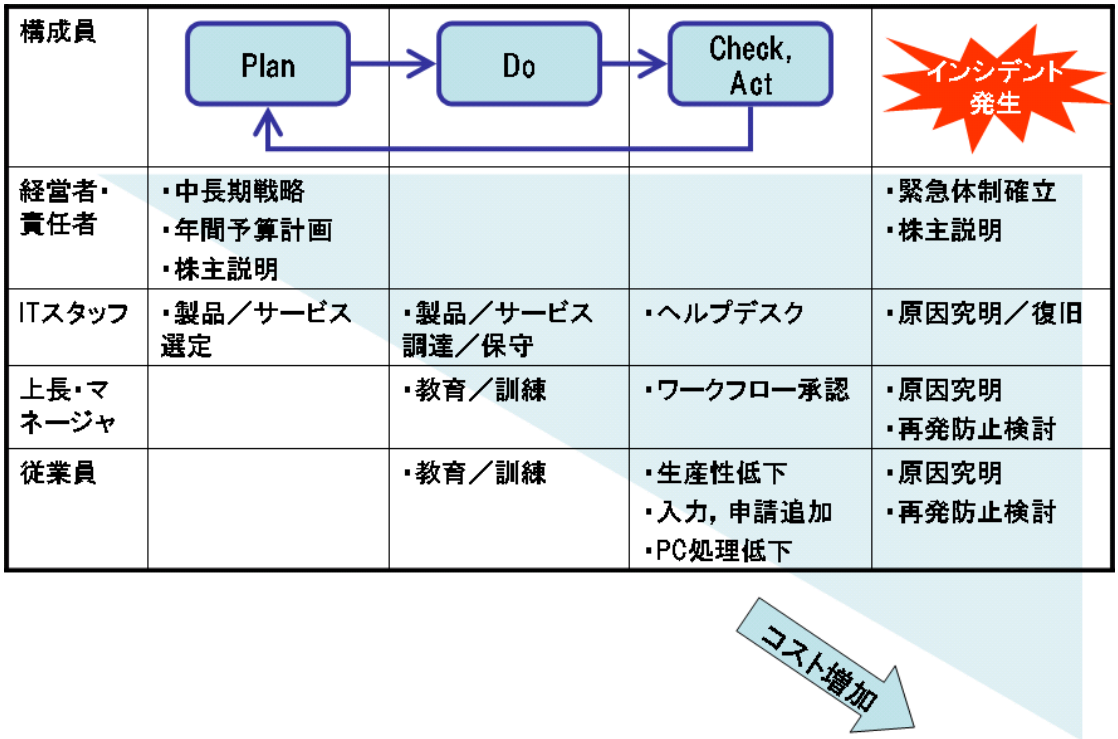

図 1.4: 企業や組織におけるセキュリティTCO

計画に関与する．行き過ぎたセキュリティ予算や，明らかに不足するセキュリティ予算とならないよう，バランスを取る必要がある．

IT スタッフは，Plan フェーズにおいて予算計画の範囲内で，目標とするセキュリティパフォーマンスを発揮できるような，セキュリティ製品やセキュリティサービスを選定する．Do フェーズで，それら製品やサービスの調達や保守を行う．さらに Check フェーズでは，セキュリティ製品やサービスの使い方やトラブルに関するヘルプデスクを行う．

上長・マネージャは，Do フェーズで自らセキュリティ教育・訓練を行うと共に，従業員に対しても実施する．Check フェーズで日々の業務におけるセキュリティ承認作業を行う．

従業員は，Do フェーズでセキュリティ教育・訓練を行うと共に，Check フェーズで日々の業務の中でセキュリティに関する入力や申請を行う．特に Check フェーズでは，例えばウイルス対策ソフトの定期スキャンなどの場合に，PC 処理低下が発生することもある．

以上が通常時のセキュリティ管理における PDCA サイクルであるが，一方，もしインシデントが発生した場合には，経営者・責任者による株主への説明から従

業員に至る再発防止策まで幅広い立場に対して，セキュリティコストが発生する．

つまり**セキュリティTCOは，上流（経営者・責任者，Planフェーズ）よりも，下流（従業員，インシデント発生時）の方が次第に増えていく**．セキュリティTCOに関して，下流のコストが上流のコストに比べてどれくらい大きいかを直接論じた文献は見当たらないが，類似する事象として，ソフトウェア開発における欠陥の修正コストに関して，文献 [9] によると，表1.2に示すように，要求開発フェーズを1とすると，運用フェーズでは68-110倍と言われている．

表 1.2: ソフトウェアの欠陥を修正するための相対コスト（出典 [9]）

誤りが発見されたフェーズ	修正のための相対コスト
要求開発	1倍
設計	2-3倍
構築	5-10倍
システムテスト，受け入れテスト	8-20倍
運用	68-110倍

ヒューマンファクタの問題が顕在化するのは，上流フェーズではなくむしろ下流フェーズである．本論文では下流（従業員，インシデント発生時）のフェーズにおけるヒューマンファクタの問題を研究範囲とする．

1.2.3 リスク定量化

セキュリティリスクを定量化する手法にはいくつか知られており，ISMS認証基準 [23, 24] では，リスクの大きさを式1.3で求めることが一般的である．

$$\text{リスク値} = (\text{情報資産の価値}) \times (\text{脅威}) \times (\text{脆弱性}) \tag{1.3}$$

情報資産の価値の評価では，情報資産の機密性，完全性，可用性が損なわれた場合の影響度を3-5段階の区分に分けることが多い．脅威の評価では，業務上の経験や過去の統計データを加味して，低い／中程度／高いの3つの区分に分けることが多い．脆弱性の評価では，情報資産の持つ弱点やセキュリティホールがどの程度であるかを加味して，低い／中程度／高いの3つの区分に分けることが多い．しかし，このようなリスク値のみでは，企業や組織におけるリスクの大きさを認識することはできても，セキュリティ対策に要する費用が適切かどうかの判断は難しい．

そこでリスク定量化の一手法として，年間予想損失額（ALE, Annual Loss Expectation）を求める手法が知られている [25,26]．ALE では式 1.4 で年間の予想損失額を計算する．

$$ALE = (\text{年間発生頻度 : 回/年}) \times (\text{1 回当たりの予想損失額 : 金額}) \quad (1.4)$$

年間発生頻度を求めるにあたり，情報セキュリティに関するインシデント発生率を表す適切なデータは現時点では見当たらない．情報セキュリティのインシデントを広くハイテク犯罪と捉えると，法務省の犯罪白書 [27] によると，ネットワーク利用犯罪の平成 22 年の検挙件数は 5,199 件であった．同年度の道路交通事故の死亡件数が 4,726 件であり，年間当たりの発生件数のオーダーとしては近い．

ただし，このような統計値は，あくまでも一般的な平均をとった値にすぎない．年間発生頻度について，もし機械などの技術的な側面だけで構成されているのなら，ある年度の結果が，次の年度の予想にも有用かもしれない．しかし，ヒューマンファクタの問題といった人間的な側面まで含めて構成されている場合，急な動機の変化も想定される．実際，米情報セキュリティ会社が 2008 年に行った調査によると，IT 管理者の 88%が「明日解雇されるとしたら，会社の機密情報を持ち出す」と回答した [28]．よって，ある年度の結果が，次の年度の予想に有用かどうかを判断することは難しい．このようにヒューマンファクタが関係するセキュリティインシデントを対象とする場合には，年間予想損失額を計算することが自体が困難であり，そのため**どれだけセキュリティ投資したらよいかどうかも分からない**．

本論文では，上記述べたようにどれだけセキュリティ投資すべきかを測ることが困難という立場に立ち，ヒューマンファクタの問題を研究範囲とする．

1.3 関連研究

1.3.1 ヒューマンファクタ

オフィスセキュリティにおけるヒューマンファクタの問題は，2000 年頃，暗号研究で著名な Bruce Schneier による著書 [29,30] の中で取り上げられた．著書 [30] では次のように説明されている．

> セキュリティの中心は人である．
>
> システムを機能させるためには一部の人を信頼しなければならない．そのような人々–信頼を託される人々–は，セキュリティシステムの一部だといえる．重要な構成要素，いや，要となる要素だといえるだろう．システムで最も靱性が高い部分であり，臨機応変の対応や即断即決ができる部分であり，攻撃者の存在を

感じとる能力が最も高い部分だからだ．しかし一方，**セキュリティシステムの構成要素として考えたとき，人間は両刃の剣である**．居眠りもすれば気がそれることもある．だまされることもある．敵側に寝返ることさえある．すぐれたセキュリティシステムとするためには，信頼を託す人の長所を活用するとともに，信頼が乱用されない防止策を講じなければならない．

また上記と同時期に，Adams らは人間は安全に振舞うように動機付けられていないことを指摘した [31]．これらの研究がきっかけとなって，2000 年以降，ヒューマンファクタに関連する数々の研究が行われてきた．

ヒューマンファクタの問題に関して多い研究は，パスワード認証つまりユーザ認証に関する研究である．パスワードは，認証手段のうち人間の記憶を頼りにした方法であることから，ヒューマンファクタの問題がつきまとう．加藤らはセキュリティ事故の原因につながる末端ユーザ（学生）のセキュリティ意識と，セキュリティ意識を左右するユーザの性格に関して調査した [32–35]．平野らはパスワードの使い回しの問題を取り上げ，マスターパスワードを保護するパスワード運用管理システムを提案した [36]．類似の研究として海外でも，Carstens らがパスワードに関連するヒューマンエラーを調査した [37]．

一方，人間はだまされることもあることから，Bowen らはフィッシングでだまされるという組織レベルでの認識率を測定した [38]．また人間がコンピュータワームの媒介を手助けする点に着目し，Sun らはユーザの行動によって感染を広げる電子メールワームに関し，ワーム拡散とヒューマンファクタを関連付けて分析した [39]．またオフィスでも特にソフトウェア開発現場において，ソフトウェアの品質を高めるために，Islam らはヒューマンファクタに焦点を当てた効果的なソフトウェアリスクマネジメントを論じている [40]．

またオフィスには，正しい権限が与えられていない者が入室するリスクもあることから，藤川らはオフィスのユニフォームを着てなりすました悪人によるインシデントを防ぐシステムを提案した [41]．さらに，正しい権限が与えられた者でも悪人によって恐喝される可能性までを考慮して，石垣らは恐喝・詐欺・故意・過失を防ぐための新たな認可手法を提案した [42]．

さらにオフィスは場所が複数箇所にまたがることもあることから，荒井らは公開可能な一般情報と, 社外に開示してはならない機密情報とが混在するコンピュータシステムにおいて, 機密情報の共有と保護を両立させる情報フロー制御モデルを提案した [43]．同様に，小野らは機密情報の持出し記録管理と, 持出し先での文書保護とを実現する, 機密情報持出し制御システムを開発した [44]．

さらには端末（PC）操作ログを集め，来歴を分析すること情報漏えいなどの危険行為を検出する方式も研究されている [45–47]．

また芝口らは，仕事量とセキュリティ対策の徹底度との関係を分析し，仕事量

が一定でない場合にその期間に採るべき対策を決定する方式を提案した [48].

以上をまとめると，ヒューマンファクタの問題に関する研究は，人間の意識や動機付けに関する心理学的なアプローチ [32–40] と，人間の振る舞いに関する技術的なアプローチ [41–48] に大別できる．

1.3.2 文書セキュリティ

オフィスで扱う文書に対するセキュリティは，オフィスセキュリティマーク認証基準 [49] や什器メーカによるファイリング術 [50] の中で総論としてまとめられている．

学術的には，石島らは，業務遂行上, 適切なその共有範囲はどのくらいか, アクセス権限の付与はどのように行なうべきかに関する，ファイリングシステムの技法を考察した [51]．三品らは，文書に付与されるメタ情報欠落問題を解決するため, オフィス文書の来歴を記録して文書に安全な形で添付する来歴封入と, そのデータ構造を提案した [52]．今井らは，情報漏えい対策機能としてユーザを特定可能な ID を電子透かしで文書に埋め込む場合に，複数のユーザが結託して異なる ID を持つ文書を比較することにより ID を改ざんする脅威に対し，結託耐性符号でユーザ ID を文書に埋め込む方式を提案した [53].

一方 Brin らは，電子データに含まれるテキスト部分に着目し，電子データの部分コピーを精度良く検出する方式を提案した [54, 55]．さらに芹田らは，テキストデータかバイナリデータかを問わず電子データの部分一致を精度良く検出方式を提案した [56].

また道井らは，印刷時にデータを暗号化し，特定の人物，場所以外での印刷物の出力を制限するシステムを開発した [57–61]．さらに金井らは，組織のセキュリティポリシーに従って紙文書と電子文書のセキュリティを確保するシステムを開発した [62].

さらに複合機の機能として，e-文書法に対応してタイムスタンプを付与する複合機が紹介されている [63]．また，地紋を用いた情報埋め込み技術を開発し，コピーガードやパスワードコピー機能を備えた複合機により，紙情報の不正な複写を禁止することが紹介されている [64].

紙文書に関して，福田らは，人工物固有の特徴を用いて認証を行う技術である人工物メトリクスの一つとして，紙から固有な値を再現性よく抽出する人工物メトリック・システムを提案した [65].

以上をまとめると，文書セキュリティに関する研究は，電子文書のみを対象とする研究 [52–55] と，紙文書までを対象とする研究 [57–65] とに大別できる．

1.4　研究の目的

本研究では，事業所（オフィス）におけるセキュリティ対策が必然的に抱える，投資とリスクのトレードオフに着目し，

- 上長・マネージャにとって，セキュリティ管理に要する時間・手間が少ないこと
- 従業員にとって，本来の業務が圧迫されないこと

を両立させるような，トレードオフ解消技術を開発することが目的である．特に従業員のヒューマンファクタが絡む情報リスクに対して，未然に防止する立場と，もしインシデント発生時の事後対応の立場から，以下の 3 点を研究テーマとする．

- （テーマ１）従業員が過失によって引き起こす情報リスクに対し，未然に防止する．
- （テーマ２）従業員が意図的に引き起こす情報リスクに対し，インシデントが発生した後に迅速に復旧する．
- （テーマ３）従業員が第三者に狙われる情報リスクに対し，未然に防止する．

このようなトレードオフ解消技術の開発により，経営者にとっても結果的に，セキュリティ投資対効果を高めることができるメリットがある．

1.5　本論文の構成

本論文の構成は，以下に述べるとおりである．まず，2 章では，ヒューマンファクタによる情報リスクを技術で低減するオフィスセキュリティの提案を述べる．3 章では,（テーマ１）に対応し，重要な印刷を検出するための，文字コード処理方式による高速な印刷コントロール機能の提案および開発結果を述べる．4 章では,（テーマ２）に対応し，端末（PC）での印刷を監視し効率的に調査を行うための，印刷監視システムの提案および開発結果を述べる．5 章では,（テーマ３）に対応し，不正プログラムから情報資産を保護するクライアント向けファイルアクセス制御方式の提案および開発結果を述べる．まとめとして，6 章では，研究全体の結論を述べ，今後の課題をまとめる．

第2章　ヒューマンファクタによる情報リスクを技術で低減するオフィスセキュリティの提案

2.1　現状分析

本節では，オフィスセキュリティを取り巻く現状を分析し，ヒューマンファクタの問題点を掘り下げる．

2.1.1　紙文書の漏えいリスク

オフィスで働く従業員が事業所で就業時間中に行う業務は，業種や部門によりその内容は異なるかもしれないが，典型的な業務の一つは「文書作成」と考えられる．実際，従業員による勤務時間中の PC 使用率は約 7 割と言われており [66]，また PC は文書作成に適したキーボードを持つため，文書作成に PC が使用されることは容易に類推できる．

作成される文書の形態の点からすると，2000 年あたりからペーパーレス化が叫ばれており，図 2.1 に示すように，紙文書は電子媒体に比べて相対的に少なくなっている [5]．しかし，事業所からの情報漏えいは，図 2.2 に示すように，2005 年の調査から常に紙媒体が 5〜7 割を占めている [6]．紙媒体により 1 回当たりに漏えいする量は，電子媒体による漏えいに比べ小さい．しかし，1 回当たりに漏えいする量が小さくても，頻度が多くなれば全量として無視できなくなる．つまり，従業員が文書作成時に自然と扱うはずである紙文書の漏えい対策が課題の一つである．さらに近年，クラウドコンピューティング環境の利用が加速することが言われており [67]，そのため電子媒体は事業所以外のデータセンターに預けることが想定されることからすると，事業所に残る紙媒体は今後ますます目立つ存在となることが予想される．

よってオフィスでの紙文書は，常に業務と密接な関係にあり，一方で漏えいリスクも非常に高い．そのため，印刷におけるセキュリティ対策としては，そもそ

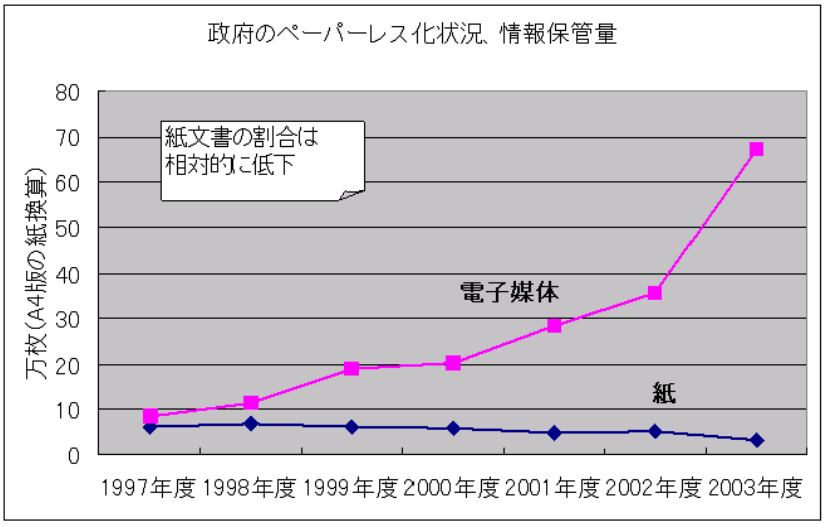

図 2.1: 情報保管量（出典 [5] のデータをもとに作成）

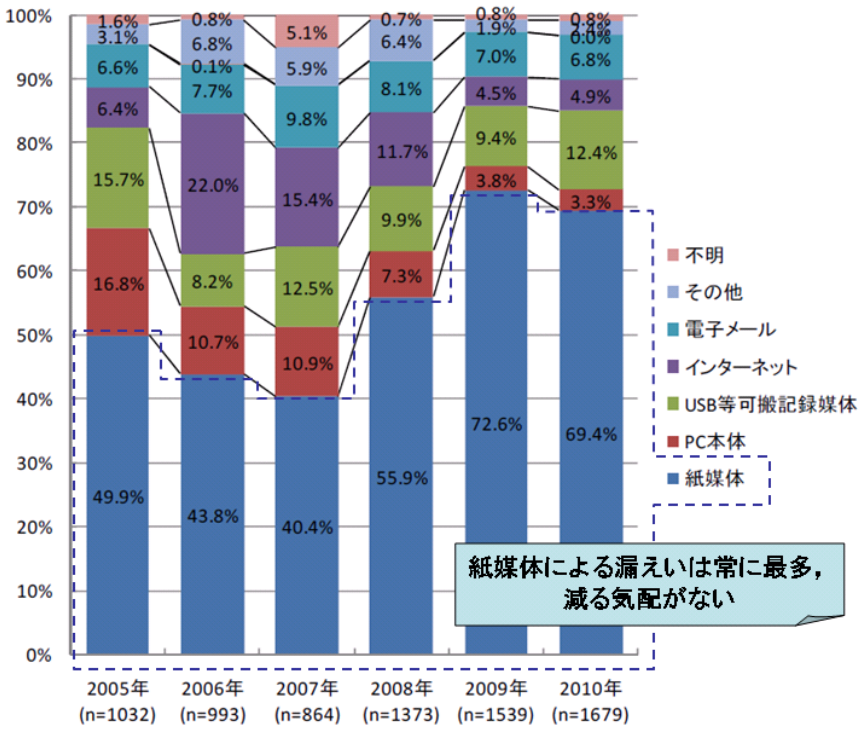

図 2.2: 漏えい経路比率の経年変化（件数）（出典 [6] の図に加筆）

もPCでの印刷を防止するための事前対策と，もし印刷した紙文書が漏えいした場合に備えた事後対策に分けて検討することが鍵である．

- （分析結果１）オフィスでの紙文書は漏えいリスクが高いため，**PCでの印刷によるデータ漏えいへの事「前」対策**が必要．
- （分析結果２）紙文書は業務と密接な関係があり，漏えいを完全になくすことは困難なため，**PCでの印刷によるデータ漏えいへの事「後」対策**が必要．

2.1.2 未知ウイルス感染リスク

従業員が持つ情報は，必然的に従業員のPCにて作成・保存されることとなる．このようなPC上に残る情報を狙う第三者となると，近年は入退室管理が普及していることからすると物理的な侵入リスクは減り，むしろネットワーク利用（Web，電子メールなど）や可搬記憶媒体の利用に伴い感染するマルウェア（コンピュータウイルス，トロイの木馬，ワームなど，malicious softwareの略）のリスクが増加している．実際，図2.3に示すように，2009年には1.5秒に1個の割合で新種のマルウェアが発生したと試算されている [7]．

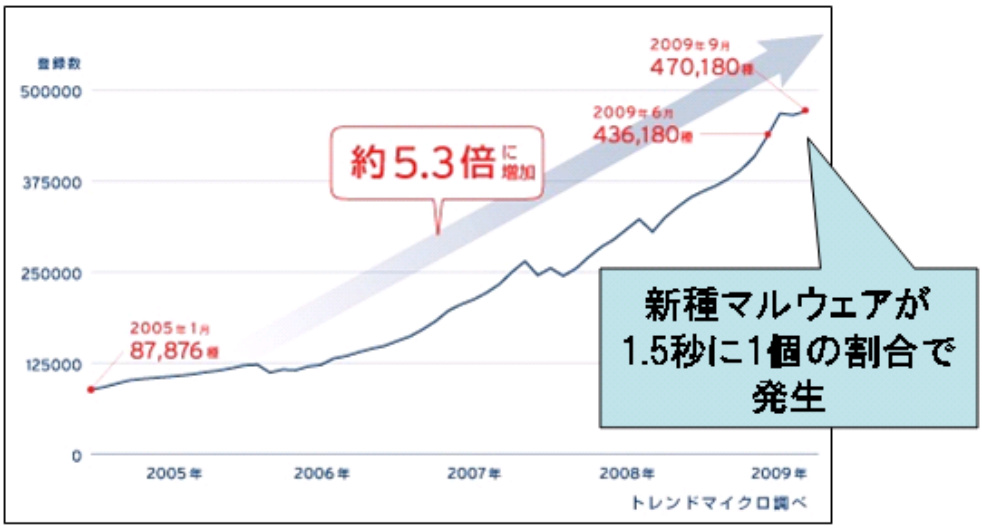

図 2.3: マルウェアの登録数（出典 [7] の図に加筆）

特に近年は，APT（Advanced Persistent Threats）と呼ばれる，ソフトウェアの脆弱性を悪用し，複数の既存攻撃を組合せ，ソーシャルエンジニアリングによ

り特定企業や個人を狙い，情報窃盗などを行うサイバー攻撃手法が問題視されている [68]．近年のサイバー攻撃の事例を表 2.1 に示す．重要情報が格納されたサーバが最終目標であるが，そのサーバにアクセスする際の踏み台として従業員の PC が狙われる可能性が高い．つまり，従業員が外部組織とのやりとりに使う PC において，新種マルウェアへの対策が課題の一つとなる．

表 2.1: 企業や官公庁を狙った主なサイバー攻撃（APT 攻撃）事例

時期	攻撃先	内容
2011 年 4 月	国内・米国 S 社	ハッカー集団「アノニマス」がネット配信サービスに不正侵入したとされる．計 1 億件の個人情報の流出が疑われた．
春	国内 I 社	情報漏えいを引き起こす危険のある**ウイルスメールを大量に受信**．
5 月	米国 C グループ	ネットバンキングシステムからカード利用者の情報が盗まれる．
6 月	米国 G 社	電子メールサービスの利用者数百人のメール内容が盗み見られる．
8 月	国内 M 社	本社や工場などのサーバと**パソコン 83 台がウイルスに感染**．
2012 年 1 月	国内 J 組織	**職員のパソコンがウイルス感染**．一部システムのログイン情報が流出．
6 月	国内 Z 省	アノニマスがホームページに不正侵入．一時的に閲覧できない状態に．

PC でウイルス対策ソフトを稼動させることは常識であるが，次々に発生するマルウェアに対してパターンファイルの開発や更新が追いつかない空白の期間が無防備になってしまうことも事実である．そのため，未知マルウェアに感染した場合に備えた封じ込め対策の検討が鍵である．

- （分析結果 3）ウイルス感染リスクが高い PC において，**PC への未知マルウェア感染によるデータ改ざん・漏えいへの対策**が必要．

2.1.3　認知科学的アプローチとその限界

セキュリティにおけるヒューマンファクタの問題に対して，認知科学的アプローチを取ることもある [18]．認知科学的アプローチでは，人間を情報システムの一部と見なして，人を入力，情報処理（認知），出力する過程をもつモデルとして理解される．認知科学的アプローチでは，ヒューマンファクタの問題を「エラー」と「違反」に分けて考える．

- エラー：意図しない結果を生み出す人の行為又は不行為．エラーはさらに，スキルベース（訓練不足），ルールベース（解釈誤り），知識ベース（緊急，複雑，未知のもの）に分類される．
- 違反：人が意図的に実施する違反行為．動機付け，信念，態度，規範，組織文化の問題が背景にある．何らかの属性（若者は年長者よりも違反が多い，など）があることが多い．

こうした認知科学的アプローチに基づき，現実のオフィスセキュリティでも，教育，訓練，ルール作りが広く行われている．印刷の漏えいリスクに対しては，印刷を許可しない文書には「印刷不可」「禁複写」などの背景文字を入れることが多い．また，未知ウイルス感染リスクに対しては，不要なアプリケーションをインストールしない，電子メールの見覚えない添付ファイルは勝手に開かない，などのルールが作られることが多い．さらには，これらのルールを徹底するために，組織に入社・加入したタイミングや年に 1 回のタイミングで，e-learning などの教育およびテストを行うことも広く普及している．

しかし，情報漏えいやウイルス感染といった情報リスクに対して認知科学的アプローチをとったのでは大きく 2 点で問題が残る．

- 従業員は，本来の業務を行うために組織に属すると考えられ，本来の業務ではないセキュリティ対策に時間を取られるのは本望ではなく，生産性を下げることにつながる．つまり，セキュリティ TCO を上げる一要因となる．
- エラーの発生頻度はハインリッヒの法則（1:29:300 の法則）が当てはまるかもしれない．一方，違反は突発的な意図により発生することが否定できず [69]，発生頻度が急激に変動しうる．そのため，セキュリティ投資をどれだけやったら良いか分からない．

2.1.4　オフィスセキュリティでよくあるエラーと違反

オフィスでは文書という情報資産を扱う一方で，従業員というヒューマンファクタまで考慮して，セキュリティを確保しなければならない．オフィスセキュリティにおいてよくあるエラーと違反をまとめると，図 2.4 に示すとおりとなる．

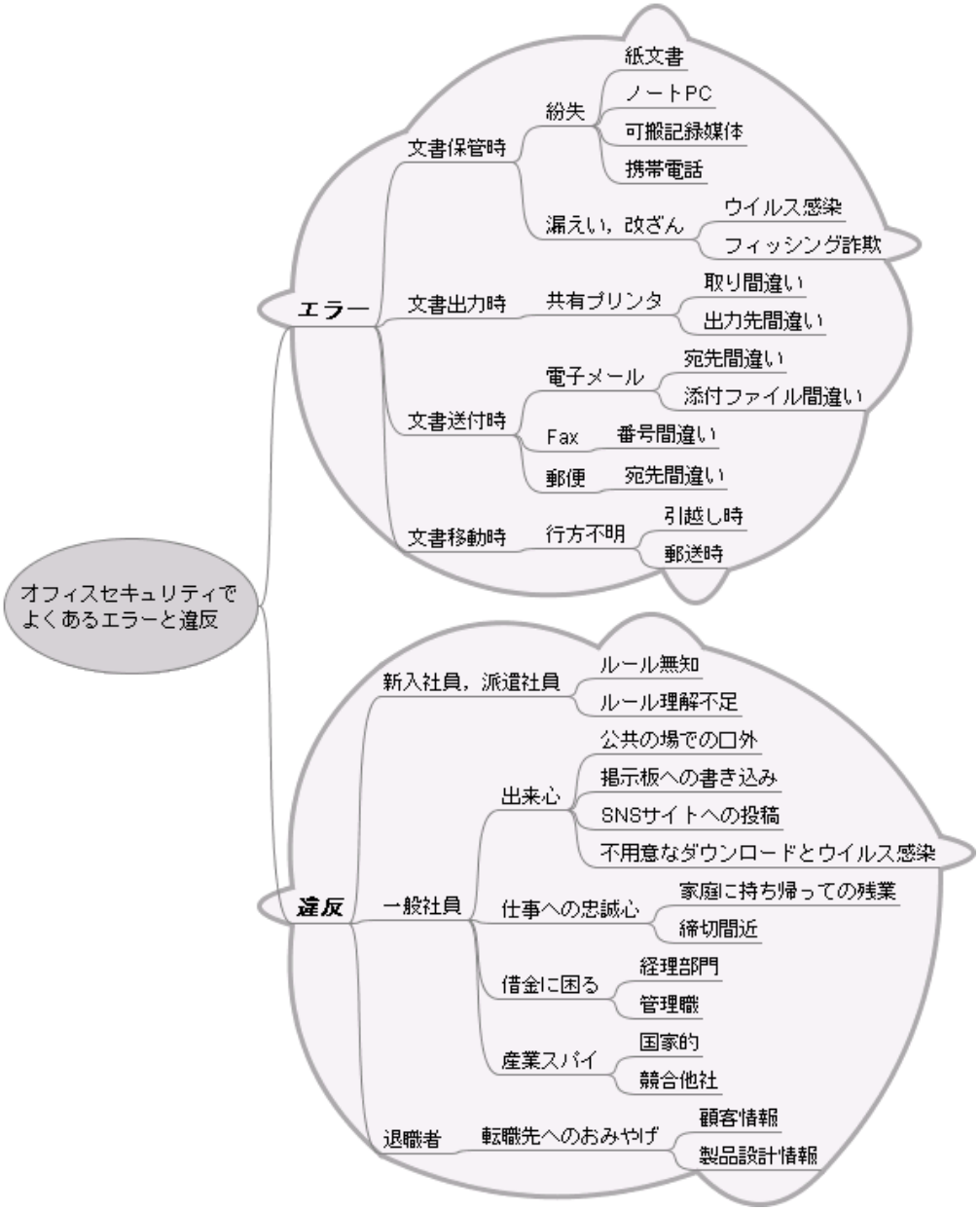

図 2.4: オフィスセキュリティでよくあるエラーと違反

エラーの観点では，オフィスで従業員が文書を扱うことから，文書の保管・出力・送付・移動といった文書のライフサイクルのあらゆる点で，紛失，漏えい・改ざん，取り間違い，送付間違い，行方不明などのリスクがある．エラーに対しては，従業員がそうしたエラーを引き起こす前に適切な気づきを得ることができれば，エラー低減に役立つものと考えられる．ただし，近年はオフィスではPCで一人一台に割り当てられ，PCが普及する以前の時代に比べて，隣の従業員でさえその行動が見えにくくなっている．エラーを引き起こす前の適切な気づきを技術で与える必要がある．

一方，違反の観点では，新入社員，派遣社員によるルールの理解不足による行為をはじめ，一般社員による出来心，仕事への忠誠心，借金などの外的要因，産業スパイといった各種の動機からくる行為や，退職者による転職先へのおみやげといった行為などのリスクがある．違反に関して，ルールの理解不足に対しては教育や訓練が重要である．実際，ほとんどの組織で導入時の集合教育や定期的な教育は広く行われている．次に，産業スパイや退職者に対しては法的措置に訴えることまで想定する必要がある．産業スパイや退職者の違反は，組織内ルールや情報システムを熟知していることが多いため，これらのリスクを低減するには，技術面以外での対策が必要である．また，一般社員による出来心，仕事への忠誠心，借金などの外的要因は，当事者の軽はずみな行動を抑止すれば，違反低減に役立つものと考えられる．こうした一般社員による軽はずみな行動も，PCが普及する以前の時代に比べて，隣の従業員でさえその行動が見えにくくなっているため，軽はずみな行動をした場合に技術で見える化を行い抑止する必要がある．

2.2 研究動機

本研究では，ヒューマンファクタによる情報リスクの問題に対して，情報リスクを技術で低減することを目標とする．ヒューマンファクタの問題を「エラー」と「違反」とに分けて考え，それぞれ次に示す方針で対処する．

- ヒューマンファクタのエラーの問題に対して，**適切な判断情報を適切なタイミングで人に提供する技術**を確立することで，エラーとなる人の行為を未然に防ぐ．
- ヒューマンファクタの違反の問題に対して，**もし違反をした場合に，その調査を効率化する技術**を確立することで，人の違反行為に対する抑止効果とする．

エラーは前述したようにスキルベース（訓練不足），ルールベース（解釈誤り），知識ベース（緊急，複雑，未知のもの）に分類される．いずれのエラーであって

も，適切な判断情報を適切なタイミングで提供することで，エラーにつながる人の行為を未然に防ぐ効果を期待できる．

一方，違反は人の意思による行為であるため，意思に訴えかける対策も有効である．そのため，いわゆる記録をとって事後調査に備えることで，意図的な行為に対する抑止を期待できる．なお，このような監視の強化と制裁により統制をとる考え方は，パノプティコン [70,71] と呼ばれる全展望監視システムと類似している．パノプティコンとは，中心が監視施設となっており，そこから周囲の全てが監視できるようになっている，円形の建物の構造である．多くの人間を一点から監視できるため，抑止効果を期待できる．

ところで，極度の監視はプライバシー侵害にもなりかねないが，オフィス（事業所）においては従業員はある程度の契約の元に業務を行うものであると考え，本研究では，監視によるプライバシー侵害は研究対象外とした．

2.3 提案するオフィスセキュリティ技術

提案するオフィスセキュリティ技術の全体像を，図 2.5 に示す．

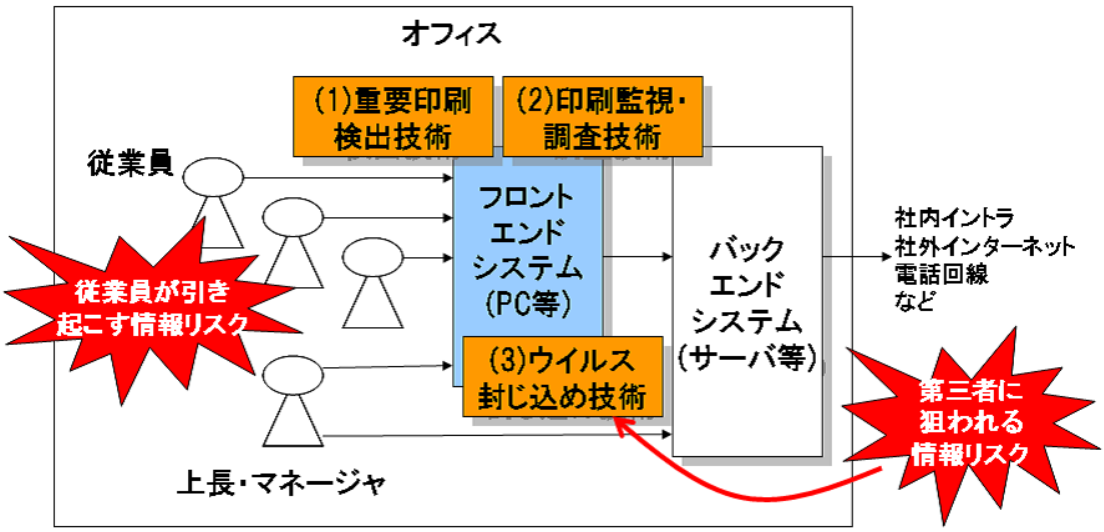

図 2.5: 提案するオフィスセキュリティ技術の全体像

(1)PC での印刷によるデータ漏えいへの事「前」対策：重要印刷検出技術
紙文書の漏えいリスクに対し，適切な判断情報を適切なタイミングで人に提供する技術を確立しエラーを未然に防ぐ．

(2)PC での印刷によるデータ漏えいへの事「後」対策：印刷監視・調査技術
紙文書の漏えいリスクに対し，もし違反をした場合に，その調査を効率化する技術を確立し違反行為に対する抑止とする．

(3)PC への未知マルウェア感染によるデータ改ざん・漏えいへの対策：ウイルス封じ込め技術
未知ウイルス感染リスクに対し，適切な判断情報を適切なタイミングで人に提供する技術を確立しエラーを未然に防ぐ．

以下，各技術内容の概要を順に述べる．

2.3.1 PC での印刷によるデータ漏えいへの事「前」対策：重要印刷検出技術

従来技術

オフィス（事業所）における PC での印刷を一律に禁止することは現実的ではなく，その一方で， PC での印刷を一旦許可してしまうと，どんな印刷でもできてしまうのが現状である．そこで近年では，印刷時に印刷データを画像化し，画像に基づく解析手法として OCR（Optical Character Recognition）を利用して印刷内容を把握する方法が知られている [72]．OCR はプリンタや複合機に内蔵される場合や，プリントサーバと連携して動作する場合がある．こうした OCR には，

- 文書 OCR：書籍や新聞など，あらかじめ形式の決まっていない印刷図書を読み取ることを目的としたもの
- 帳票 OCR：提携業務に即されて作られた，あらかじめ決まった形式の帳票や伝票を読み取ることを目的としたもの

の 2 種類が知られており，業務で作成する文書を読み取るには前者の文書 OCR が適当である．そうした文書 OCR は主な処理として「レイアウト解析」「文字解析」を行う必要があり，文書の識別には時間がかかる傾向にある．そのため文書 OCR を使った印刷内容を識別するのでは，適切な判断材料を適切なタイミングで利用者に提供する上で，レスポンス良く印刷内容を判断することが困難であった．

研究課題

印刷時にレスポンス良く印刷内容を識別することが課題である．レスポンスの良さを維持するには，従来技術であった文書 OCR の利用や，文書 OCR をプリン

タや複合機，プリントサーバで利用することには，処理に時間がかかる点で限界がある．そこで，本研究では，文書 OCR を使わずに，PC での印刷時にプリンタドライバで文書の内容を把握する技術を確立する方針とした．

PC での印刷時にはプリンタドライバで「レイアウト配置」「文字出力」を行う．もし文書 OCR を使って印刷内容を識別するには，文書 OCR では「レイアウト解析」「文字解析」を行うことからすると，図 2.6 に示すように，印刷内容を把握するまでにレイアウトに関する処理が重複していることに気付いた．そこで，プリンタドライバでレイアウト処理をスキップしつつ「文字出力」のみを高速に抽出する方針とした．

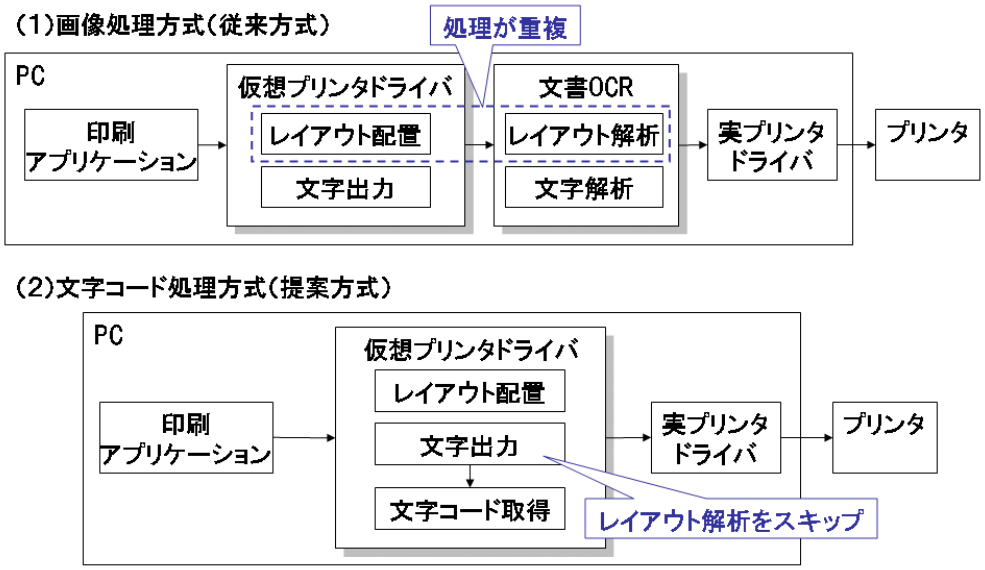

図 2.6: 重要印刷検出技術：従来方式の課題と提案方式の特徴

研究成果

印刷時にプリンタドライバとして動作し，さらに文字出力のみをデバイスドライバのフッキング技術で取得し，キーワードチェックを行う文字コード処理方式を備えた仮想プリンタドライバを開発した．本仮想プリンタドライバは Windows XP 上で動作する．文字解析の正確さの点では，文書 OCR に比べて小さな文字や装飾文字なども間違いなく取得できることを確認した．レイアウト解析の影響の点では，途中に改行があっても複雑な段組みを除き，連続して文字を取得できることを確認した．さらに，日本語特有の横書き・縦書きなどであっても連続して文

字を取得できることを確認した．高速性の点では，文書 OCR が A4 で 1 ページ当たり約 2 秒を要し，ページ数が増加するほど正比例して時間がかかるのに対し，提案方式では 1 ページ当たり最大 0.4 秒を要し，ページ数が増加しても最初の 1 ページ目に余計に時間がかかるだけであることを確認した．

このため，提案方式の仮想プリンタドライバを事業所の各 PC にインストールし通常の文書作成を行えば，上長・マネージャはあらかじめ NG ワードを指定しておくだけで印刷禁止を徹底することができる．また一方で，従業員にとっては印刷時間が大きく増加することはなく，さらに間違って NG ワードが含まれる印刷を行うことが未然に防止される効果もある．

本研究成果の詳細を 3 章で述べる．

2.3.2 PC での印刷によるデータ漏えいへの事「後」対策：印刷監視・調査技術

従来技術

もし情報漏えいが発生すると，何が漏れたか，他に漏れた情報はないか，誰が漏らしたか，などの調査が行われる．情報漏えい発生後のインシデント・レスポンスを支える技術として，デジタルフォレンジック[1)]が知られている [4]．とくに印刷物による漏えいが発覚した場合には，調査員は，印刷に使われたと疑われる PC の，下記の場所を組み合わせて調べることとなる．

- レジストリキー：プリンタドライバをインストールした形跡があるか
- イベントログ：いつ何を印刷した形跡があるか
- スプールファイル：印刷イメージが残っていないか

しかし，デジタルフォレンジック技術を適用する上では，何を印刷したかを知ることはイベントログにファイル名の一部などしか残っていないことから確実とは限らない問題や，数多くの PC を対象に管理者権限で情報を収集する必要があることから時間がかかるといった問題を抱える．

従来，印刷に関する監視技術として，課金目的あるいは環境負荷軽減目的で，ユーザが何枚印刷したのかをカウントする技術は広く普及している．しかし，印刷枚数をカウントするだけでは，上記のような情報漏えい発生時の調査には役立たない．

[1)] デジタルフォレンジックとは，デジタルデータに対する鑑識技術のことであり，不正アクセスや機密情報漏洩などコンピュータに関する犯罪や法的紛争が生じた際に，原因究明や捜査に必要なデジタルデータの証拠保全および調査・分析を行うとともに，デジタルデータの法的な証拠性を明らかにする一連の科学的手法・技術を言う．

研究課題

デジタルフォレンジック技術は，情報漏えいが発生してから調査を開始するために，確実とは限らない，時間がかかるといった問題がある．とくに漏えいが発覚した後に所定の期間内に何らかの報告責任が生じる場合も多く，その際には数多くの調査員を投入して，期間内に証拠を探し出す必要がある．そこで通常の業務を行う段階から事前の備えを実施することで，印刷物による漏えいが発覚しても，何が漏れたか，誰が漏らしたかを正確に効率良く絞り込めるようにすることが課題である．

研究成果

印刷時に仮想プリンタドライバでテキスト情報を取得すると共に，テキスト情報だけでは欠落してしまうレイアウト情報や図形・写真などを考慮し，印刷イメージのサムネイル画像として取得する，図 2.7 に示すような，分散型の印刷監視システムを考案した．印刷物による情報漏えいが発生した場合には，テキスト情報を使って検索し印刷ログの絞り込みを行い，サムネイル画像を目視確認して漏えいした印刷物との一致性を特定する．

デジタルフォレンジック技術で調査対象となるスプールファイルの場合，印刷元の電子ファイルに比べてそのサイズが約 1.85 倍になるのに対し，提案方式の印刷ログでは印刷元の電子ファイルに比べてわずか 0.04 倍程度で済む．そのため印刷の証拠となりうるデータのサイズを約 97.4%削減することができる．さらに，1 週間以内に一次報告を行う漏えい調査シナリオを想定した場合に，従来のフォレンジックプロセスで約 4 名を要していた作業工数が，1 名で実施可能な見通しを得た．

このため，提案方式の印刷監視システムを事業所に導入し通常の文書作成を行えば，上長・マネージャは，いつ，誰が，何を印刷したかを正確かつ効率良く調査できる．一方で，従業員にとっては印刷ログデータの一時保管やネットワーク転送で業務が圧迫される可能性は小さくなる．

本研究成果の詳細を 4 章で述べる．

2.3.3 PC への未知マルウェア感染によるデータ改ざん・漏えいへの対策：ウイルス封じ込め技術

従来技術

もし PC がマルウェアに感染すると，マルウェアは PC 上の「ファイル」「レジストリ」「キーストローク」「表示画面」「スピーカ／マイク／カメラ」「モデム」「ネッ

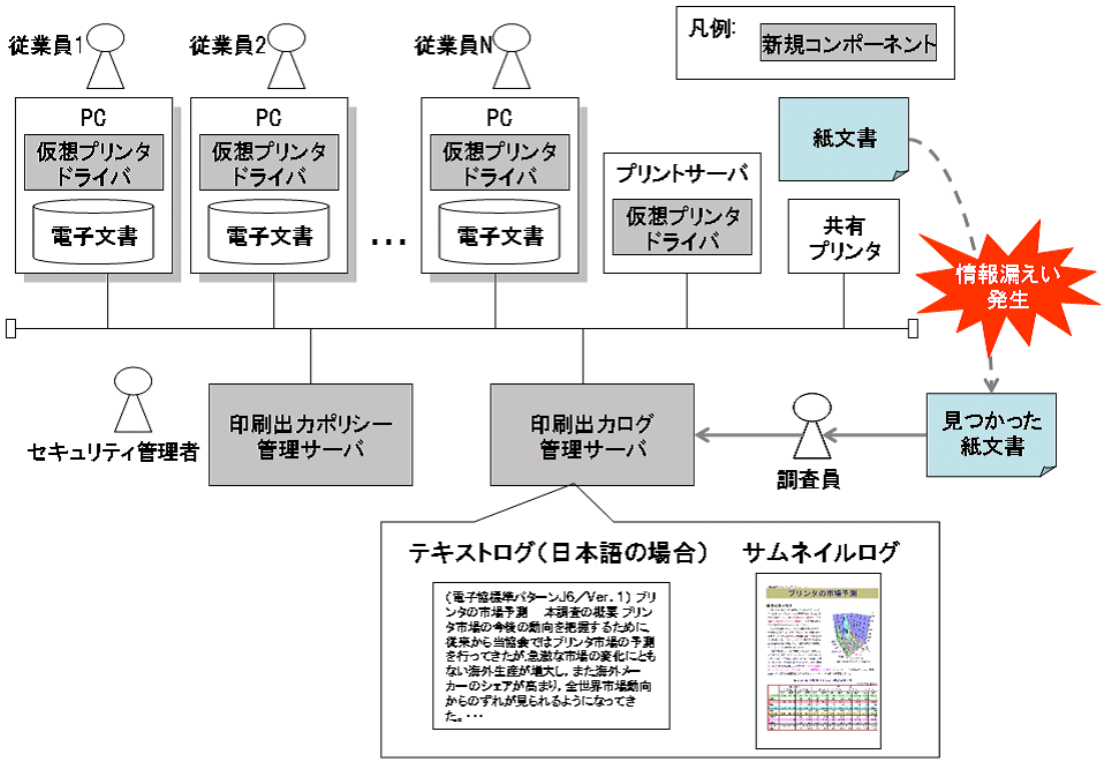

図 2.7: 印刷監視・調査技術：印刷監視システムの全体像

トワークインタフェース」「プリンタリソース」などに様々な悪影響を及ぼす．この中でも機密性，完全性の点から特に狙われやすい資産は「ファイル」である．

こうしたマルウェアを検出・駆除するために従来使われてきたアプローチが，表 2.2 に示すブラックリスト型であるが，近年は新種マルウェアの出現にパターンファイル更新が追いつかないことから，ホワイトリスト型のウイルス対策 [73–76] も次第に注目を集めつつある．

ホワイトリスト型のアプローチとしては大きく，

- あらかじめプログラムを登録しておき，未登録のプログラムの実行を禁止する（プログラム実行禁止方式）
- あらかじめプログラムとファイルの対応関係を登録しておき，未登録のプログラムからのファイルアクセスを禁止する（ファイルアクセス制御方式）

の 2 通りに分類できる．組み込み機器（例えば DVD レコーダなど）のような固定的な使い方をする PC ではプログラム実行禁止方式が有用である一方，事業所に

表 2.2: ブラックリスト型とホワイトリスト型の比較

比較項目	ブラックリスト型	ホワイトリスト型
方式の説明	悪意のあるプログラムの特徴を事前に定義し，その特徴に合致するプログラムや振る舞いを検出・防止	安全が認められたプログラムの特徴を事前に定義し，その特徴に合致しないプログラムや振る舞いを検出・防止
利点	過去のマルウェアを全て検出可	新種マルウェアも検出可，パターンファイル更新が不要
欠点	新種マルウェア検出のためパターンファイル更新が常に必要	PCの使い勝手が下がる（正規のアップデートに制限など）

おけるPCではプログラムの追加・削除が頻繁に起きることが想定されるため，後者のホワイトリスト型のファイルアクセス制御方式が有用である．

このようなホワイトリスト型のファイルアクセス制御のポリシーを設定するにあたっては，従来，実際にプログラムやサービスを走行させて発生したアクセス履歴をもとに設定する方式 [77] が知られている．しかし，多用途に使われることの多いPCでは，走行すべきプログラムやサービスが多岐にわたり，手間がかかる問題がある．

研究課題

多用途なPCに対し，ホワイトリスト型のファイルアクセス制御ポリシーを確実かつ簡易に設定することが課題である．とくに従業員はPCに関する専門知識（プログラムのパスなど）を持たないことも予想されるため，ポリシー設定に必要な知識も少ないことが望ましい．

研究成果

PCで想定される操作と利用プログラムを洗い出し，実際にプログラムを走行させて正常アクセスをパターン化した．その結果，大きく3パターンに分類できることが判明した．

1. 関連付けアプリケーションからのファイルアクセス

2. OLE（Object Linking and Embedding）対応のアプリケーションからのアクセス

3. 用途別プログラム（シェル，ウイルス対策，ファイル共有など）からのファイルアクセス

上記パターン化した正常アクセスを PC 毎に設定するため，OS の持つ管理情報（レジストリ，インストール情報など）を読み込み，図 2.8 に示すような，ホワイトリスト型ポリシーを自動生成するポリシー設定支援ツールを開発した．

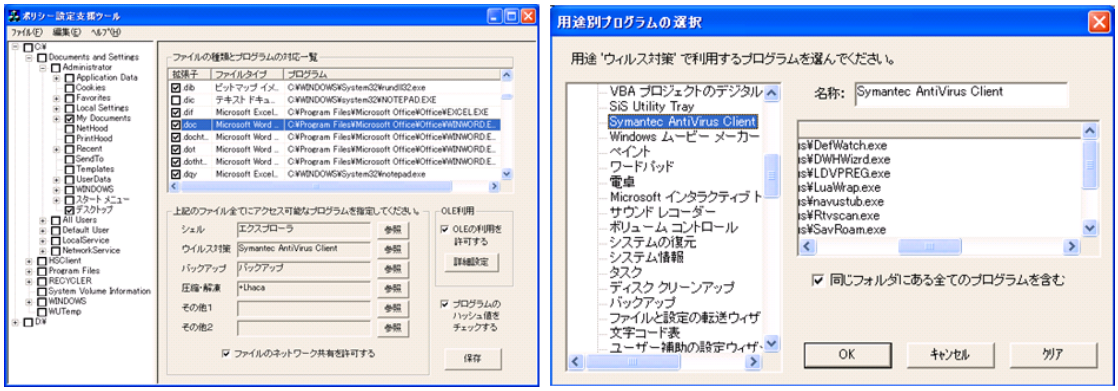

図 2.8: ウイルス封じ込め技術：ポリシー編集画面（左），用途別プログラムの選択画面（右）

インタフェースを定量的に評価する方法の一つである GOMS 法（Goals, Operations, Methods and Selection rules）[2] [78] を適用したところ，初期ポリシーの設定を 10 分以内の操作で完了できる見通しを得た．またポリシー設定に必要な知識も，データフォルダの位置，重要データの拡張子，PC で使っているアプリケーション名だけで済むことを確認した．

このため本ポリシー設定支援ツールを使って PC にホワイトリスト対策を実施すれば，上長・マネージャにとっては確実なポリシー設定を期待できる．一方，従業員にとっては簡易な操作により数分程度でポリシー設定を完了することができる．

本研究成果の詳細を 5 章で述べる．

[2] GOMS 法とは，ユーザビリティ評価手法の一つであり，インタフェースの操作をキーストロークやマウス操作まで分解し，各段階でかかる時間を予測する方法のこと．

第3章　文字コード処理方式による高速な印刷コントロール機能の開発

3.1　はじめに

企業や組織における情報セキュリティ対策として，オフィスの情報漏えい対策は重要な取り組むべき課題である．オフィスとは「組織が業務のために利用する建屋又は居室等」と定義されており [49]，つまり，入退室管理で区切られた，特定の業務を行う役割が与えられた従業員の作業場所である．このようなオフィスで取り扱う文書は，紙文書も電子文書も両方存在することが通常であり，電子文書から紙文書に印刷するためのプリンタもオフィスに備えられることも多い．近年，企業で生成される文書の 93%が電子文書であると言われる [79] 一方で，企業からの情報漏えい経路として，紙文書が 69.4%と最多である [6]．つまり，生成量として少ない紙文書の方が，漏えいの主な原因になっているのが現状である．これら紙文書の生成は，業務の IT 化の進歩により，電子文書から印刷出力されることが多いと予想されるため，情報漏えい対策の一環として，印刷出力のセキュリティ強化は重要である．

本章では，印刷出力のセキュリティ強化を目的とし，印刷内容を高速で判定可能とする印刷コントロール機能の開発について述べる．

3.2　既存セキュリティ技術

3.2.1　印刷セキュリティ対策

印刷セキュリティ対策は，情報漏えい対策の一環として，およそ（1）予防対策,（2）検出対策,（3）フォレンジック対策に大別できる．

まず（1）予防対策は，印刷しても情報漏えいにならないよう未然に防止する対策である．予防対策の例としては，印刷自体を防ぐ場合 (1a)〜(1c) と，印刷内

容を加工する場合 (1d)(1e) がある．

- (1a) プリンタドライバのインストールを，OS セキュリティ機能で禁止する．
- (1b) 電子文書を開くアプリケーションのセキュリティ機能で印刷を禁止する [80, 81]．
- (1c) 印刷権限のある人のみが IC カードをかざすことで印刷できるようにする．
- (1d) あらかじめ電子文書の一部を墨塗りする [82]．
- (1e) 電子文書の必要な部分をモザイク状に暗号化し，権限のある人のみが復号して閲覧できるようにする [83]．

次に（２）検出対策は，漏えいされたとしても印刷出力結果から漏えいを見つける対策である．検出対策の例としては，あらゆる電子文書にあらかじめ検出のための特徴情報を付与しておき印刷時に特徴情報も印刷する場合 (2a) と，印刷時に印刷出力結果に特徴情報を付与する場合 (2b) がある．

- (2a) 電子文書のヘッダやフッタ，背景文字などに，出所（Copyright など），機密レベル（極秘，社外秘など），取扱い方法（持ち出し厳禁，印刷不可など）を記述する [84, 85]．
- (2b) 印刷時に，ヘッダやフッタ，背景文字などに，機密レベル，取扱い方法などをプリンタドライバで追加して印刷する．

最後に（３）フォレンジック対策は，もし漏えい事故が起きたとしてもその被害拡大や復旧コストを最小に抑える対策である．フォレンジックの対策の例としては，事故発生後の調査 (3a)(3b) と，事故発生後の調査を確実化・効率化するための事前対策 (3c) とがある [86]．

- (3a) 流れるネットワークパケットを監視することで，漏えいの兆候を把握する．ネットワークフォレンジックと呼ばれる．
- (3b) 漏えいが疑われる利用者の PC から決定的な証拠を探し出す．コンピュータフォレンジックと呼ばれる．
- (3c) 印刷文書ごとに異なる ID 情報を電子透かしとして挿入し，事故後に，漏えいした紙文書からその ID 情報を抽出し，いつ，誰が，何を印刷したかを追跡する．

さらには，前述の（１）予防対策と（２）検出対策とを組み合わせたような，3.2.2 項に述べる新たな印刷コントロール方法も知られるようになってきた．

3.2.2 DLP (Data Loss Prevention)

情報漏えい対策として，近年，DLP と呼ばれるセキュリティ製品が注目を集めている [87, 88]．DLP は，印刷出力に限らず，メール転送，USB メモリ書き出し，Web アップロードなどの様々な漏えい経路に対してコントロールを行うことができる．

DLP を実現するアーキテクチャ（以下 DLP 機構と呼ぶ）の全体像を図 3.1 に示す．DLP 機構では，まず管理者が「分類条件登録」と「コントロールポリシー登録」を行う．分類条件とは，例えば「最重要書類」「個人情報（を含む）」機密情報扱い」などに該当する文書の条件を登録し，それ以外の文書を「区分なし」と見なす，といったものである．コントロールポリシーとは，例えば「防止」「（管理者への）アラート」「（利用者への）警告」「ログ記録」といったコントロールの種類を，分類条件ごとにそれぞれ定義したものである．

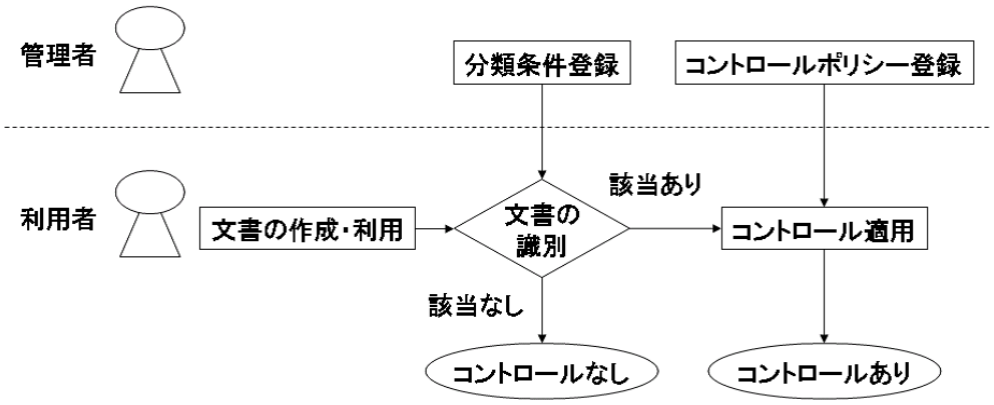

図 3.1: DLP 機構

次に利用者は業務を遂行するために「文書の作成・利用」を行う．同時に DLP 機構は，どの分類条件に合致するかを判定する「文書の識別」と，文書に対しポリシーに従ったコントロールを行う「コントロール適用」を行う．本機構の特徴は,「文書の識別」という検出対策と,「コントロール適用」という予防対策の組み合わせにより，分類条件に合致する場合にのみ，コントロールポリシーを適用する点にある．

このような文書の識別のためには，3.2.1 項の検出対策で述べた，電子文書に付与された特徴情報を見つけることで識別することもできる．しかし，こうした特徴情報は利用者の目に見えるため，悪意のある利用者が特徴情報を削除することや，別文書に一部コピーすることで特徴情報の検出を容易に回避されるおそれも

ある．そこで，文書の内容からその特徴を抽出する，フィンガープリント技術と呼ばれる手法が知られている．こうしたフィンガープリント技術は，文書中に含まれる文字列を取り出し，登録された文書との類似度を測るものである [54, 55].

3.2.3 本研究の貢献

DLP 機構を実現するには，文書の識別とコントロール適用を，どう組み合わせるかが鍵となる．なぜなら，文書の識別を実現しやすい個所と，コントロール適用を実現しやすい個所とが必ずしも一致するとは限らないからである．文献 [6] によると，情報漏えい経路として上位 5 経路だけで全体の 9 割以上を占め，その内訳は多い順に「紙媒体」「Web・Net」「USB 等可搬記録媒体」「Email」「PC 本体」である．これらの主要な情報漏えい経路に対して，DLP 機構を実現するには，表 3.1 に示す文書の識別方法およびコントロール適用方法の組み合わせが考えられる．

表 3.1: 情報漏えい経路と文書の識別・コントロール方法

情報漏えい経路	文書の識別方法	コントロール適用方法
紙媒体	画像ベース解析	印刷制御，複写制御，スキャン制御
Web・Net	HTTP 解析，ネットワークプロトコル解析	送信制御，受信制御
USB 等可搬記録媒体	ファイルベース解析	外部媒体（USB，CD-R 等）書き出し制御
Email	SMTP 解析，MIME 解析	送信制御，受信制御
PC 本体	ファイルベース解析	コピー制御，ファイル検出

ここで文書の識別に関して，ネットワークプロトコル解析やファイルベース解析であればデジタル処理可能であるため実現しやすい．一方，文書の識別を画像ベースの解析で行うことはアナログ処理が残ってしまうため，DLP 機構を実現するにあたって，精度と処理速度の点で不利な立場にある．

本稿は，従来の画像ベース解析の代替手段として，精度と処理速度を向上させた文書の識別方法を提案するものである．これにより，利用者が電子文書を印刷する時に，その印刷内容に応じて，許可，禁止，アラート，警告，ログ記録，電子透かし挿入などを行うことを目的とする．

3.3　印刷コントロールの従来技術

3.3.1　印刷環境の現状

オフィスにおける主要な業務の一つは印刷であり，印刷速度は年々向上していることは明らかである．

どの程度向上しているかを検証するため，国内主要プリンタメーカ 5 社が 1995 年から 2009 年にかけて販売したプリンタ 254 機種を対象に，A4 モノクロ印刷で，1 分当たり印刷可能な枚数を調べた．販売開始年度ごとの印刷速度の平均値をヒストグラムに示した結果を図 3.2 に示す[1)]．販売開始年度と印刷速度とを回帰分析したところ，重相関係数 R=0.91 が得られ，年々1.61 枚／分の割合で早くなっていることが判明した．印刷コントロールを行うには，こうした印刷速度を落とさないことが必要である．

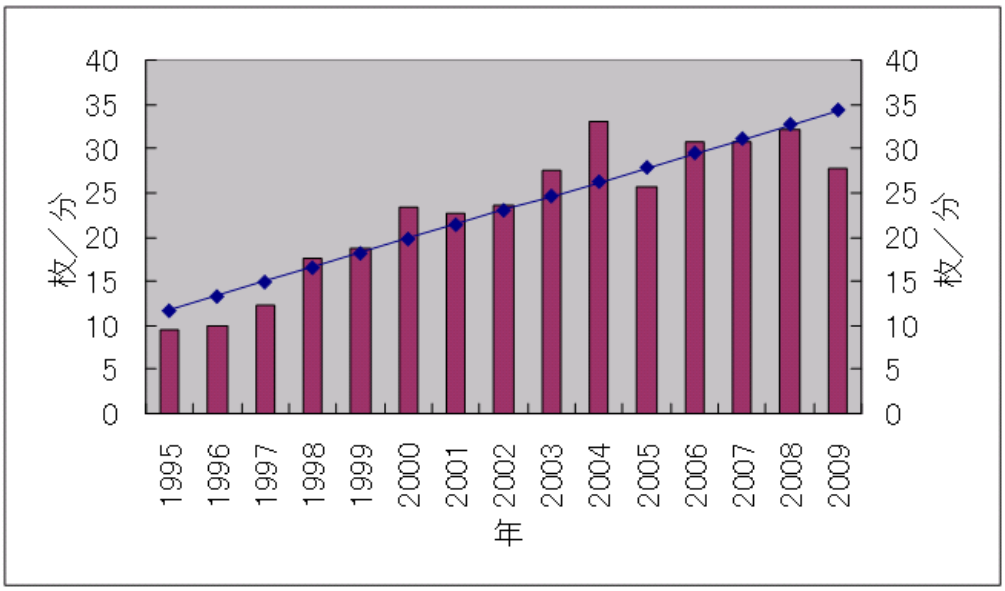

図 3.2: 印刷速度の向上（A4 モノクロ印刷）

3.3.2　画像処理方式による文書の識別

紙媒体の文書を識別するには，画像ベース解析として OCR (Optical Character Recognition) の利用が多い．実際，文献 [72] では印刷時に OCR を利用して印刷

[1)] 2009 年の印刷速度の平均が 2008 年の平均よりも遅くなっている理由の一つに，印刷速度を落として低価格化を狙ったプリンタの数が増えたことが挙げられる．

内容を把握する複合機が公開されている．本稿では，OCR を利用した文書の識別方法を画像処理方式と呼ぶことにする．OCR はその用途により 2 種類に大別できる [89, 90]．

- 文書 OCR: 書籍や新聞などあらかじめ形式の決まっていない印刷図書を読み取ることを目的としたもの．文書のレイアウトを自動的に解析，理解することで，表や文章と図や写真を自動的に分離して読み取ることが可能
- 帳票 OCR: 定型業務に即されて作られた，あらかじめ決まった形式の帳票や伝票を読み取ることを目的としたもの

オフィスにおける印刷文書は多様であるため，その文書を識別するには，文書 OCR の利用が適当である．この文書 OCR の処理動作は，その特徴からすると「レイアウト解析」と「文字解析」に大別できる．

- レイアウト解析: 画像全体から文章・表・図の範囲を区別する，文章についてその範囲や縦書き・横書きを区別するなど，文書のレイアウト情報を得る
- 文字解析: 使用言語を区別する，フォントや文字装飾（太字，斜体，下線，カラー，白黒反転など）の差異を吸収して文字だけを識別する，文章解析により誤検出文字を補正するなど，文字情報を得る

とくにレイアウト解析と文字解析は互いに独立した処理ではなく，文字解析の前提に必ずレイアウト解析が必要である．そのため画像処理方式は文書の識別に時間がかかる傾向にある．

3.3.3 仮想プリンタドライバによる印刷コントロール

オフィスにおけるプリンタは，様々な機種のプリンタが使われるのが通常であるため，プリンタ機種に依らない印刷コントロールが望まれる．そうした印刷コントロールを実現するために従来技術として仮想プリンタドライバによる方式が提案されている [91]．本方式では，あらかじめ利用者の PC に仮想プリンタドライバをインストールしておき，業務で印刷する時には，利用者はアプリケーションから仮想プリンタドライバを呼び出して印刷操作を行う．すると，仮想プリンタドライバが印刷履歴取得や電子透かし挿入などのコントロールを行った後，その仮想プリンタドライバから実プリンタドライバを呼び出して，通常の印刷を行う．本方式のメリットは次に示すとおりである．

- 利用者がアプリケーションから印刷する操作性が既存の操作性と変わらない

- 現在利用しているアプリケーションやプリンタを継続利用できる
- 仮想プリンタドライバの出力は汎用性が高い Bitmap ファイルであり，どのような実プリンタドライバでも印刷連携できる

さらに同文献 [91] によると，利用者が印刷アプリケーションから直接実プリンタドライバを呼び出すことでコントロールを回避するという攻撃に対する対策も述べられている．

この仮想プリンタドライバ方式では Bitmap ファイルに出力できるために，その出力を文書 OCR の入力とし，文書 OCR の結果を受けて文書を識別する，という連携は可能である．しかし，このような連携では，依然として 3.3.2 項の画像処理方式で述べたように，文書の識別に時間がかかる傾向にある．

3.3.4 課題

印刷コントロールにおける DLP 機構を実現するには，以下の 2 つの方向性がある．

- 文書の識別方法として，画像処理方式（従来方式）を改良する．
- 文書の識別方法として，従来方式とは異なる別のアプローチを採用する．

いずれの方向性も重要であるが，前者のアプローチでは 3.3.3 項で述べたようにアナログ処理が残り，文書の識別に時間がかかるという問題が残る．そこで，本稿では後者のアプローチを取ることにした．つまり，本稿における課題は，**画像処理方式とは異なる方式で，印刷コントロールとして高速に文書を識別する方法を確立すること**である．

3.4 文字コード処理方式による文書の識別

3.4.1 プリンタドライバでの文字コード処理

プリンタドライバとは，アプリケーションが印刷時に呼び出し，プリンタへの印刷出力のために使用されるドライバである．プリンタドライバの処理動作は，その特徴からすると「レイアウト配置」と「文字出力」に大別できる．

- レイアウト配置: どのページの，どの位置に配置するかなどを決める

- 文字出力: 印刷フォント，サイズ，カラー，装飾などを決めて文字を出力する

とくに文字出力では，図 3.3 に示すように，電子文書に含まれる文字コードの集まりを，紙文書に印字する文字の形に変換する処理を行う．例えば電子文書中の「あ」は「U+3042」という文字コードで表されており，プリンタドライバによる処理で印刷時に,「あ」という文字の形に変換されることになる．3.3.3 項で述べた仮想プリンタドライバの場合には，プリンタ用言語の代わりに Bitmap ファイルに出力される．

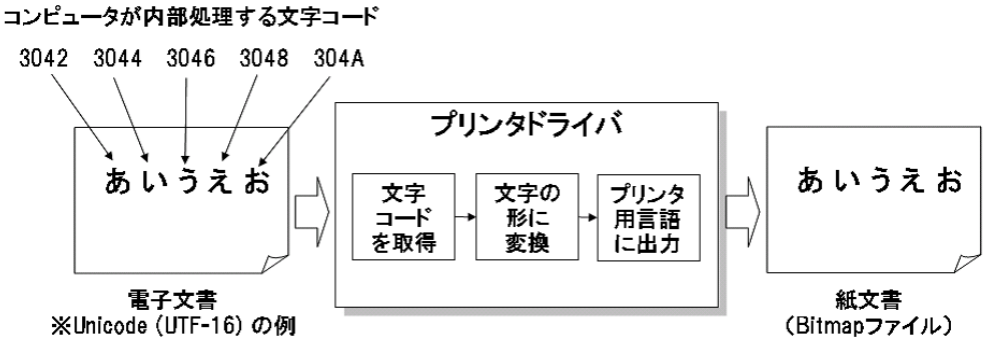

図 3.3: 文字出力処理の概要

文書を識別するのに仮想プリンタドライバと文書 OCR を組み合わせた画像処理方式（従来方式）の場合には，図 3.4 の（1）に示すように，仮想プリンタドライバでレイアウト配置した画像情報を，文書 OCR でもう一度レイアウト解析し直すという処理となる．文書の識別において重要なのは，レイアウト情報よりも文字情報の方であり，そのため画像処理方式で文書を識別することは，レイアウト配置とレイアウト解析が重複している．そこで，図 3.4 の（2）に示すように，仮想プリンタドライバの中で，レイアウト配置する前に出力文字を文字コードとして取得することができれば，文書の識別にかかる時間を短くできると考えた．こうした考えにもとづき，仮想プリンタドライバで文字を取得し文書を識別する方式を，文字コード処理方式（提案方式）と呼ぶことにする．

3.4.2 Windows XP 上での実装

Windows XP 上で文字コード処理方式を実装した．Windows XP ではプリンタドライバでの処理は，擬似コードで表すと図 3.5 に示す通りとなる [92]．文書全体の処理（DrvStartDoc〜DrvEndDoc），ページ単位の処理（DrvStartPage〜DrvSendPage），ページ内のレンダリング処理に大別できる．

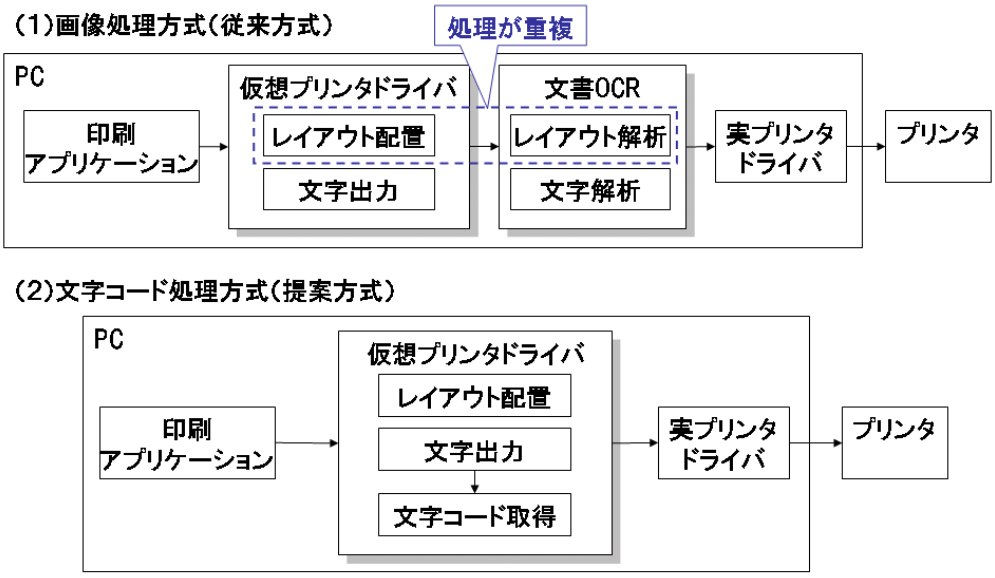

図 3.4: 文字コード処理方式

擬似コード:印刷処理

```
DrvStartDoc()                  // 文書の印刷の開始
For each physical page {
   DrvStartPage()              // ページの印刷の開始
      Rendering operations     // レンダリング処理；レイアウト配置，文字出力
   DrvSendPage()               // ページの印刷の終了
}
DrvEndDoc()                    // 文書の印刷の終了
```

図 3.5: プリンタドライバ処理の擬似コード

これらの各処理で呼ばれる関数 DrvStartDoc，DrvStartPage などに対し，OS により DDI (Device Driver Interface) Hooking と呼ばれるフッキング処理が提供されている．フッキング処理を利用すると，印刷処理における各種制御情報の参照や変更が可能となる．DDI Hooking 処理可能な関数の一つが，レンダリング処理で呼ばれる DrvTextOut である．DrvTextOut 関数の内部では，図 3.6 に示すようなレイアウト配置と文字出力の情報を取得・参照できる．

- レイアウト配置: rclBkGround 変数が文字の配置（境界矩形の上下左右のピ

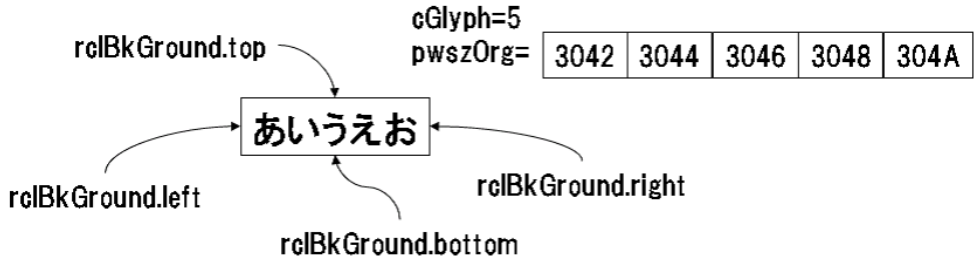

図 3.6: レイアウト配置と文字出力の例

クセル位置）を表す

- 文字出力: cGlyph 変数が文字の数を表し，pwszOrg 変数は文字コード（Unicode 文字コードあるいは Glyph（印刷フォント）文字集合）を表す．なお，Unicode と Glyph は相互に変換可能である．

文字コード処理方式の考え方は，3.4.1 項で述べたようにレイアウト配置する前に出力文字を取得することである．そこでページ単位の処理（DrvStartPage〜DrvSendPage まで）において，レイアウト情報は全て無視することとし，文字出力情報をページ内の処理順番の通りにつなげ，ページのフルテキストとして取得することとした．さらに文字は全て Unicode に統一した．

3.4.3 フィジビリティ検証

文字コード処理方式では，仮想プリンタドライバでレイアウト配置を無視し，出力文字をその処理順番の通りに文字列としてつなげるために，処理の高速化が可能となる．しかし反面，文字出力が連続して処理される間はその順番通りに文字列としてつなげることができる一方で，連続して処理されない場合は正しく文字列として取得できない可能性が考えられる．もし正しく文字列として取得できないと，キーワード検索や正規表現などでヒットできなくなる．

そこで，通常の業務で頻繁に使われると考えられる MS-Word，MS-Excel，MS-PowerPoint の 3 つのアプリケーションを対象にテスト文書を作成し，その文書を文字コード処理方式で印刷する時に，正しく文字列を取得できるかどうかをフィジビリティ検証した．フォント，装飾，サイズ，カラーを変えて文字解析を行った結果を表 3.2 に，段組みや縦書きと横書きなどのレイアウトを変えてレイアウト解析を行った結果を表 3.3 に示す．

表 3.2: フィジビリティ検証結果（１）文字解析

検証項目		MS-Word 2003 ファイル	MS-Excel 2003 ファイル	MS-PowerPoint 2003 ファイル
フォント	MS P ゴシック	○	○	○
	MS 明朝	○	○	○
	HGP ゴシック E	○	○	○
装飾	太字	○	○	○
	斜体	○	○	○
	下線	○	○	○
	囲み線	○	—	—
	網掛け	○	—	—
	上付き	○	○	○
	下付き	○	○	○
	取り消し線	○	○	○
	隠し文字	×	—	—
	影付き	—	—	○
サイズ	標準	○ (10.5pt)	○ (11pt)	○ (18pt)
	最小	○ (8pt)	○ (6pt)	○ (8pt)
	1pt	○	○	○
カラー	黒	○	○	○
	赤	○	○	○
	白	○	○	○
	白黒反転	○	○	○

○：成功，×：失敗，—：関係なし（機能なし）

まず文字解析の結果，装飾の「隠し文字」を除きすべての検証項目で文字列の取得に成功した．特に，文字のサイズが 1pt や文字のカラーが白といった，通常 OCR では文字列の取得が困難な場合にも，確実に文字列を取得できることを確認した．ところで「隠し文字」はそもそも文字列が印刷されていないため，取得できないことは当然である．

次にレイアウト解析の結果，背景文字の「透かし」を除いてすべての検証項目で文字列の取得に成功した．特に,「コメント」や「グラフ」といった複雑なレイアウトを含む文書であっても，そこに含まれる文字列を確実に取得できることを

表 3.3: フィジビリティ検証結果（2）レイアウト解析

検証項目		MS-Word 2003 ファイル	MS-Excel 2003 ファイル	MS-PowerPoint 2003 ファイル
段組み	1 段組み	○	○	○
	2 段組み	○	—	—
	3 段組み	△ [*1]	—	—
縦書きと横書き	横書き＋上向き	○	○	○
	横書き＋左向き	○	—	—
	縦書き＋左向き	○	○	○
	縦書き＋上向き	○	—	—
	縦書き＋右向き	○	○	○
罫線	3 × 3 サイズ	○	○	△ [*2]
図形描画	テキストを挿入	○	○	○
ヘッダとフッタ	ヘッダ	○	○	—
	フッタ	○	○	○ [*3]
コメント	テキスト記述	○	○	○
背景文字	透かし	×	—	—
変更履歴	テキスト記述	○	—	—
グラフ	グラフタイトル	—	○	—
	X 項目軸	—	○	—
	Y 数値軸	—	○	—
	系列名	—	○	—
	値	—	○	—
印刷オプション	スライド	—	—	○
	ノート	—	—	○
	配布資料	—	—	○

○：成功，△：一部失敗，×：失敗，—：関係なし（機能なし）
[*1] 各段の右端で折り返された最下行を 2 回重複して取得
[*2] 最下行セルの右端で折り返された最下行を 2 回重複して取得
[*3] スライドマスタ

確認した．ところで，背景文字の取得が失敗した理由は，埋め込む文字列の設定はテキストで行う一方で，MS-Word ファイルへの貼りつけは画像で行われるためと考えられる．また，表 3.3 によると文字列の取得には成功するものの，右端で折り返しにより最下行に位置する文字列が 2 回重複して取得されることで，不自然な分断に見える項目が MS-Word ファイルの「3 段組み」と MS-PowerPoint ファイルの「罫線」で部分的に認められた．重複して取得されるために，キーワード検索や正規表現で重複してヒットする可能性があるが，少なくともヒットに失敗することはない．

以上のフィジビリティ検証結果からすると，実用上はほぼ問題ないと考えられる．

ところで，文字コード処理方式は，本節で述べたように，通常の業務で頻繁に使うと考えられる文書に対して，その印刷時に精度良くフルテキストを取得できる．しかし，その一方で，プリンタドライバで文字コード処理を行わないような文書を印刷する場合には，フルテキストを取得できない．このような文書には，手元にあるファイルで実験したところ，画像ファイル（Bitmap ファイル，JPEG ファイル，TIFF ファイル等），PDF ファイルがあることが判明した．特に PDF ファイルは，業務で MS-Word などで作成した文書を PDF 化して印刷するケースも多く，対応が必要である．

そのため，実際のオフィスに適用するためには，文字コード処理方式と共に，従来方式である画像処理方式との併用を考慮する必要がある．例えば，最初に文字コード処理方式でフルテキスト取得を試し，取得できたテキストが少なすぎる場合に，画像処理方式を試す，といった併用が考えられる．よって併用の場合にも，時間のかかる画像処理方式を使うかどうかを，高速な文字コード処理方式で判定することが有効となる．

3.4.4 文書の識別例

（1）個人情報を含む文書の識別例

文書からフルテキストを取得すると，そのフルテキストを自然言語解析することで文書を識別可能である．ここでは識別の一例として，3.2.2 項で述べた DLP 機構として，文書が個人情報を含むかどうかを判定することとした．

個人情報の定義は個人を特定できる情報であり，文献 [6] によると氏名が 95.6%と多い．そこでフルテキストから氏名（姓あるいは名）を抽出するために，形態素解析ツール「茶筌」[93] を利用した．茶筌で姓あるいは名を判定するための辞書を調べると，日本人の姓と名を合わせて 32,193 語を持つことが判明した，これは日本全人口の 96.27%以上にあたる [94] ため，十分な辞書のサイズであると考えた．

ところで，形態素解析ツールは氏名でないにも関わらず氏名と誤検出する可能性がある．さらに，文書当たり個人情報を少量のみ含む場合であれば，大量に含む場合に比べて許容できるかもしれない．そこで，しきい値として 1 ページ当たり 10 名以上の氏名が含まれていれば，その文書を個人情報と判定することにした．

システム構成の全体を図 3.7 に示す．プロトタイプ開発したのは，印刷時にフルテキストを取得する仮想プリンタドライバと，形態素解析ツールを呼び出して氏名の数をカウントする自然言語処理サービスである．

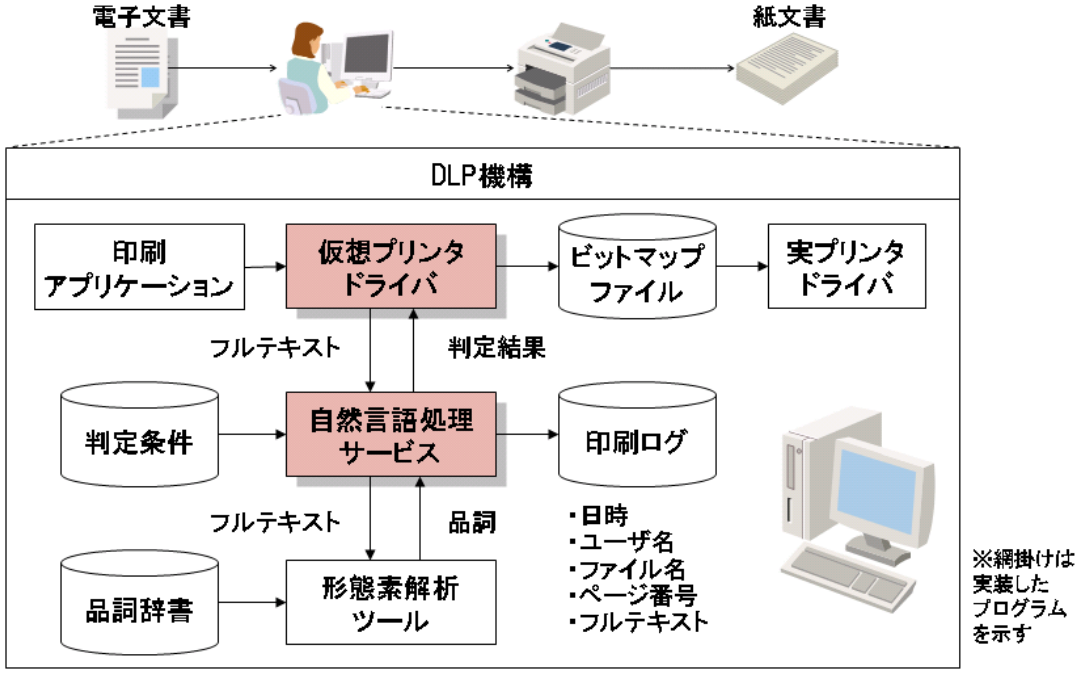

図 3.7: 個人情報を検出する印刷コントロール機能

筆者の手元にあった報告書ファイル（MS-Word の 1 ファイル）と名簿ファイル（MS-Excel の 1 ファイル）を対象に，文書の識別を試したところ，名簿ファイルのみを個人情報と判定できることを確認した．

さて上記プロトタイプでは，1 ページ単位での自然言語処理を行うこととしたが，この場合にはページをまたがる単語は認識できない．ただしこのような制限を設けたとしても，名簿などに含まれる固有名詞について，わざわざページをまたがって作成することは通常業務ではほとんどないと考えられる．

（2）「最重要書類」「機密情報扱い」等の文書の識別例

オフィスにおける情報漏えい対策として,「最重要書類」「機密情報扱い」などの機密レベルや取扱い方法などを，電子文書のヘッダや背景文字に記載することは広く知られている．文字コード処理方式は，文書の本文の他にも表 3.2 からするとヘッダに含まれる文字列もフルテキストの一部として取得できるが，背景文字の文字列は取得できない．そのため提案方式では，電子文書の機密レベルや取扱い方法などの文字列がヘッダに含まれるならば，それらを印刷時に取得し，文書の内容に応じて印刷禁止などのコントロールを行うことにも応用できる．ただし，背景文字の文字列は取得できないため，実運用上は少なくとも文書のヘッダ部に機密レベル等を記載する必要がある．

3.5 高速性の評価

3.5.1 実験方法

文字コード処理方式は画像処理方式に比べて，文書からフルテキストを取得する時間が短いことが特徴である．そこで両方式を使って文書を印刷する場合を比較することにした．印刷時間の比較方法を図 3.8 に示す．ここで印刷時間を分けて検討するために，下記に示す変数を定めた．

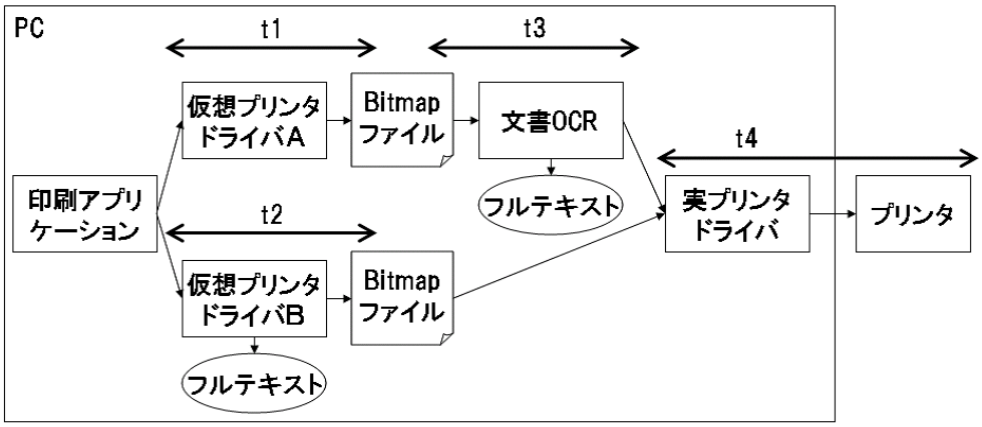

図 3.8: 印刷時間の比較方法

- t1：Bitmap 出力のみを行う仮想プリンタドライバ A による印刷時間

- t2：Bitmap 出力とフルテキスト取得を同時に行う仮想プリンタドライバ B による印刷時間
- t3：文書 OCR により Bitmap ファイルからフルテキストを取得する時間
- t4：Bitmap ファイルを実プリンタドライバで印刷する時間

従来方式である画像処理方式による印刷時間 Ta は，Ta=t1+t3+t4 で表わされる．提案方式である文字コード処理方式による印刷時間 Tb は，Tb=t2+t4 で表わされる．さて，t4 は実際のプリンタによる印刷時間であるが，レーザプリンタやインクジェットプリンタといったプリンタの種類によって大きく異なり，さらに Ta と Tb で共通して出てくるため，本評価では t4 を除いて考える方針とした．印刷を行う PC の測定環境を表 3.4 に示す．

表 3.4: 測定環境

項目	スペック
ハードウェア	VMware Player 3.0 を利用して構築
CPU	Intel Core2 Duo 2.2GHz
メモリ	512MByte
HDD	20GByte
OS	Windows XP Professional SP3

仮想プリンタドライバ A と仮想プリンタドライバ B は，プロトタイプ開発した．文書 OCR は，文書 OCR 製品を 2 種類（A 社製 2005 年版，S 社製 2005 年版）比較したところ文字認識時間が倍近く違ったことから，高速な A 社製 2005 年版を採用した．印刷する文書には，実際の業務で作成した A4 サイズで 5 ページの MS-Word 文書を用意した．当文書に含まれる文字数は，1 ページ目 1,861 文字，2 ページ目 1,615 文字，3 ページ目 2,064 文字，4 ページ目 1,556 文字，5 ページ目 1,851 文字である．

また時間測定方法は，ストップウォッチを使って次に示すレスポンス時間を 5 回ずつ測定し，その平均を計算した．

- t1，t2 は，MS-Word アプリケーションで印刷ボタンを押下してから， MS-Word アプリケーション表示領域の右下に印刷中に出るプリンタのアイコンが消えるまでを目視で確認した．
- t3 は，A 社製の文書 OCR で，文字認識を開始するボタンを押下してから，文字認識完了後に出てくる結果画面が表示されるまでを目視で確認した．

3.5.2 実験結果

印刷ページ数を増やしながら時間を測定した結果を表 5 に示す．フルテキスト取得時間だけに要する時間は，従来方式では t3，提案方式では t2-t1 で表わされる．提案方式は従来方式に比べて，フルテキスト取得に 0.1〜0.4 秒という短い時間で処理が完了している．さらに，印刷ページ数が増加していったとしても，フルテキスト取得時間も同様に増加することは認められなかった．よって，提案方式によるフルテキスト取得時間が印刷時間に比べて十分に小さいことが確認できた．また印刷に要する時間は，従来方式では t1+t3，提案方式では t2 で表わされる．この t2 は t1+t3 に比べ，表 3.5 に示すように，61〜66%という高速性を達成している．

表 3.5: 印刷時間の測定結果

印刷ページ数	t1（秒）	t2（秒）	t3（秒）	t2 / (t1+t3)（%）
1	2.4	2.7	2.0	62
3	7.0	7.1	4.5	61
5	11.3	11.7	6.6	66

3.5.3 考察

文字コード処理方式におけるフルテキスト取得時間は，3.5.2 項で述べたように，印刷ページ数が増加していったとしても，フルテキスト取得時間も同様に増加することは認められなかった．これは，OS のマルチタスク処理により，最初の 1 ページの印刷に余計に時間がかかるだけで，次ページの印刷以降はフルテキスト取得時間が印刷全体時間に吸収されるためであると考えられる．

また文献 [95] によると，レスポンスタイムとして利用者がシステムの反応が瞬時に行われていると感じる限界は 0.1 秒であり，利用者の考えの流れが妨げられない限界は 1.0 秒であると言われている．従来方式では，表 3.5 によるとフルテキストの取得に数秒以上のレスポンスタイムの増加が見込まれることから，利用者が印刷が遅くなることに気付くと考えられる．一方，提案方式では，3.5.2 項で述べたようにフルテキストの取得に 0.1〜0.4 秒ほど増加するだけであり，そのため利用者にとって印刷が遅くなることにほとんど気付かないと考えられる．

3.6 おわりに

本稿では，印刷コントロールに関する DLP 機構の実現に向け，文書の識別を高速化するために，従来方式の画像処理方式とは異なるアプローチで，プリンタドライバにおける処理で文字情報を取得する文字コード処理方式を考案した．さらに，文字コード処理方式を実現するプリンタドライバを Windows XP 上で実装し，そのフィジビリティ検証および印刷速度への影響を評価し，実用上，問題のないことを確認した．

提案方式である文字コード処理方式は，既存オフィス環境に導入する上で，プリンタやプリントサーバを変更・追加設置することなく，プリンタドライバだけで文書の識別を行うために，SOHO (Small Office/Home Office) といった小企業でもオフィスの情報漏えい対策として容易に導入できるセキュリティ対策である．

今後の課題は，下記に示す通りである．

- 文字コード処理方式で取得したフルテキストを使いつつ，実際の業務で使われる各種文書に対応した文書の識別手法を確立すること．
- 印刷コントロールとして，印刷禁止，アラート，ログ取得，出力プリンタ切り替え，電子透かし挿入などとの連携を図ること．

第4章　効率的なフォレンジック調査のための印刷監視システムの開発

4.1　はじめに

企業や組織が直面する数あるセキュリティ事故の中で，情報漏えいは最も深刻な事故の一つである．企業や組織からの情報漏えい経路として，紙文書による漏えいはここ数年ずっと最多であり，2005 年には約 5 割だったのに対し 2010 年には約 7 割を占めている [6].

情報漏えいが発生すると漏えいに企業や組織が自らすぐに気付くわけではなく，現実には実際の漏えいからその発覚までにタイムラグがあり，第三者による発見が契機となり発覚までに数週間から数ヶ月以上かかるといわれている [96]．その間にも生成される紙文書は大量である．実際，企業や組織におけるコピー用紙の使用量を調べ [97,98]，職員数で割ると，平均して職員 1 名当たり年間約 3,000 枚近くの使用量にのぼることが判明した．したがって，業務で生成される大量の紙文書の中から情報漏えいにつながった証拠を見つけるデジタル・フォレンジック（以下，フォレンジックと略す）調査は，手間と時間を要する作業となる．

オフィスからの情報漏えい経路は，紙文書以外にも，電子メール，外部媒体，Web が知られている [6]．電子メール，外部媒体，Web を経由して漏えいが起きた場合には，フォレンジック調査手法として各種のログや PC に残されたデータを使って，いつ，誰が，何を漏えいしたかの絞り込みが行われる [86,99–101]．一方，紙文書を生成する印刷に対するフォレンジック調査に関しては，従来ほとんど取り上げられなかった．

そこで本章では，オフィスでの印刷が情報漏えいにつながる事故に焦点を当て，印刷を対象とするフォレンジック調査を効率化するためのプロセスを提案すると共に，プロセス実現に向けた支援システムの開発結果とその評価を述べる．本章の構成は以下の通りである．4.2 節で主要な情報漏えい経路に対する従来のフォレンジックプロセスを述べ，4.3 節で絞り込みを効率化するための拡張フォレンジッ

クプロセスを提案する．4.4 節で提案プロセスを実現するための印刷監視システムの開発結果を紹介し，4.5 節でフォレンジック調査の効率性に関する評価結果を述べる．

4.2 従来のフォレンジックプロセスの概要と課題

本章ではデジタル・フォレンジックを，プロセス（手順）面と，手法面に分けて概要を述べ，本稿で扱う課題を整理する．

4.2.1 フォレンジックプロセス

フォレンジックプロセスとは，調査対象を PC，サーバ，携帯電話などに限定せず，広くデジタルデバイスが関係する犯罪を対象に，現場からの証拠押収，保管，解析，最終的な報告までを進めるためのリファレンスとなる手順である．これまでにもいくつかのフォレンジックプロセスが提案されてきており [102–105]，プロセスの各フェーズの細分化レベルや，各フェーズで使われる用語が異なるのが現状である．本稿でのフォレンジック調査手順は，その中で広く知られていると考えられる米 NIST によるフォレンジックプロセス [105] を参考にした．本手順は次に述べるように，調査対象が，媒体，データ，情報，証拠へと次第にエスカレーションする点が特徴である．

(1)Collection（媒体の収集）
　特定の事象や犯罪に関連するデータの識別，媒体へのラベル付け，記録，収集を行う．

(2)Examination（データの保全）
　データの完全性を保護しつつ，収集されたデータから関連する情報を識別し，抽出する．

(3)Analysis（情報の解析）
　前記 Examination の結果を分析することで，特定の事象や犯罪に関する疑問（例えば 5W1H）を解決するのに役立つ情報を導き出す．

(4)Reporting（証拠の報告）
　前記 Analysis の結果及び実施したプロセスを報告する．

4.2.2 フォレンジック調査手法

フォレンジック調査手法は，犯罪の種類や，犯罪に使われたデジタルデバイスの種類などによって，利用する手法が大きく異なる．オフィスからの主要な情報漏えい経路 [6] である紙文書（印刷），電子メール，外部媒体，Web を取り上げただけでも，フォレンジック調査で扱う対象は表 4.1 に示すように多岐に渡り，そのため調査手法も幅広い知識と技術が必要となる．

表 4.1: 情報漏えい調査で扱うフォレンジック対象の例

情報漏えい経路	Collection（媒体の収集）	Examination（データの保全）	Analysis（情報の解析）	Reporting（証拠の報告）
紙文書（印刷）	クライアント PC プリントサーバ プリンタ/複合機	レジストリ イベントログ スプールファイル 印刷ログ	いつ，誰が， 何を印刷したか	報告書
電子メール	クライアント PC メールサーバ メールアーカイブ	メール格納ファイル 削除メール メール送受信ログ	いつ，誰から， 誰に，何を送信/受信したか そのメールは既読か	報告書
外部媒体	外部媒体 PC/サーバ 外部媒体書き出し管理サーバ	レジストリ 削除ファイル 外部媒体書き出しログ	いつ，誰が， 何を使い，何をコピー/移動したか	報告書
Web	クライアント PC Proxy サーバ	レジストリ キャッシュ アクセスログ	いつ，誰が， どの Web サイトで，何をしたか	報告書

Collection では，オフィスでの作業の中心は PC 操作であることから，疑わしい職員が所有する PC を物理的に押収する．あるいは，電子メール利用におけるメールサーバや Web 利用における Proxy サーバなどの何らかの集中管理ノードに目をつけ，完全コピーを行う．

Examinationでは，職員が証拠を隠滅する可能性を考慮し，集中管理ノード上のログや職員が意図しなくともPC上に自動的に残されるデータ（レジストリ，キャッシュなど）の回収を行う．あるいは，職員が意図的に削除したデータの復元などを行う．

Analysisでは，データを分析する専用フォレンジックツール [106,107] などを利用し，データのファイルタイプやタイムスタンプなどによって仕分けしつつ，データ同士の関連性をタイムライン分析などによって明らかにし，5W1Hの疑問に答える情報を導き出す．

Reportingでは，専用フォレンジックツールを使って報告書の作成やプレゼンテーションを行う．

主要な情報漏えい経路のうち，電子メールやWebによる経路の場合，メールサーバやProxyサーバなどの集中管理ノードを経由して行われると共に，職員が集中管理ノード上の自らの履歴を自在に消すことが困難であるため，集中管理ノードをCollection対象とすることは自然な流れである．また外部媒体による漏えいは，レジストリに過去にPCに接続した外部媒体の種類や型番などが全て記録されているため，疑わしい職員が使ったPCのレジストリを調べることで使用した外部媒体を特定することは常套手段である．しかし，印刷による漏えいの調査にあたっては，次項で述べるように状況が異なる．

4.2.3 印刷フォレンジック調査の課題

印刷による漏えい時には，集中管理ノードであるプリンタや複合機，プリントサーバの出力する印刷ログから調べるのが自然である（図4.1中のプリンタ/複合機と印刷ログデータ）．通常のオフィスでは，環境負荷削減のためにコピー用紙の使用量を通じて印刷枚数の管理は行っていても，印刷内容まで管理することはほとんど行われていないのが現状である．更に，プリンタや複合機はオフィスで共有する機器だけでなく個人で所有するプリンタの場合もあるため，フォレンジック調査のためには，印刷命令を出したPC側を調査することも考慮しなくてはならない（図4.1中のPC）．そのため一つ目の課題は，**PCにまでCollection対象が広がるためにPC押収工数が，職員数やオフィスの分散化に応じて大きくなること**である．

また，PCを対象とするExaminationでは，レジストリキー（図4.1中のレジストリデータ）を調べることで使用プリンタが判明し，イベントログ（図4.1中のイベントログデータ）を調べることで印刷履歴が判明し，更にスプールファイル（図4.1中のスプーラデータ）を調べることで印刷イメージが判明する．しかし，印刷履歴には印刷ジョブ名しか記録されないために，本当にどの文書が印刷されたか

を特定することは困難である．特に職員が悪意をもってファイル名を変更して印刷した場合には，印刷履歴から元ファイル（図 4.1 中の文書データ）をたどることは困難となる．更に，スプールファイルは印刷に成功すると削除されることが通常のため，数週間から数ヶ月以上前の印刷イメージを復元することはほぼ不可能である．そのため二つ目の課題は，**印刷に関して Examination で抽出可能なデータの品質が低く，Analysis に有用な情報の引き出しが困難なこと**である．

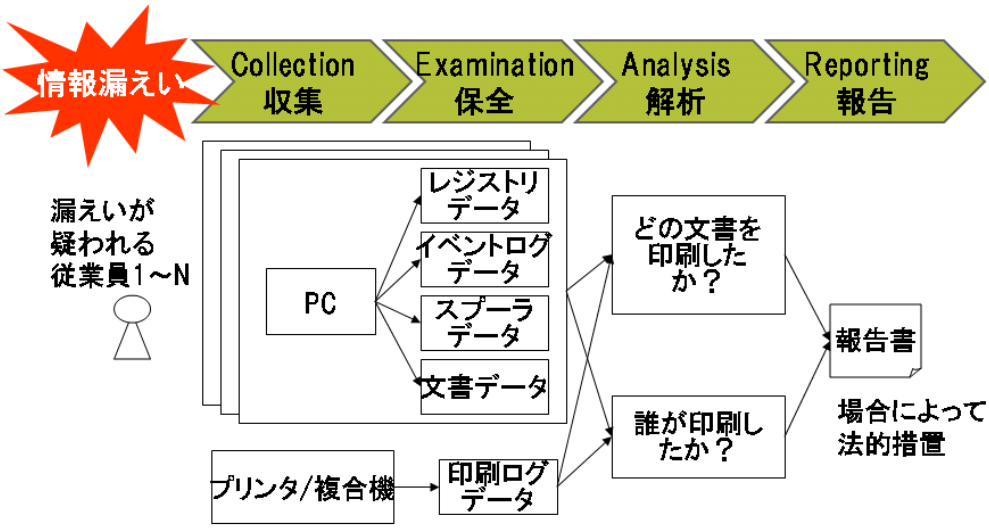

図 4.1: 従来のフォレンジックプロセスによる漏えい調査

4.3 拡張フォレンジックプロセスの提案

4.3.1 解決方針

従来のフォレンジックプロセス，つまり 4.2.2 項で述べたような PC 押収，HDD データコピー，専用ツールによる解析，報告というプロセスでは，印刷による情報漏えいが発覚してからフォレンジックプロセスを開始していた．そのため，後からいくらフォレンジック調査手法を駆使しても，漏えい調査を遂行することは 4.2.3 項で述べたように困難であった．そこで図 4.2 に示すように，情報漏えいが発覚する以前，つまり日常的な業務における Monitoring（印刷の監視）フェーズを新たに加えれば良いと考えた．従来のフォレンジックプロセスに Monitoring を加えた手順を，以下，拡張フォレンジックプロセスと呼ぶ．

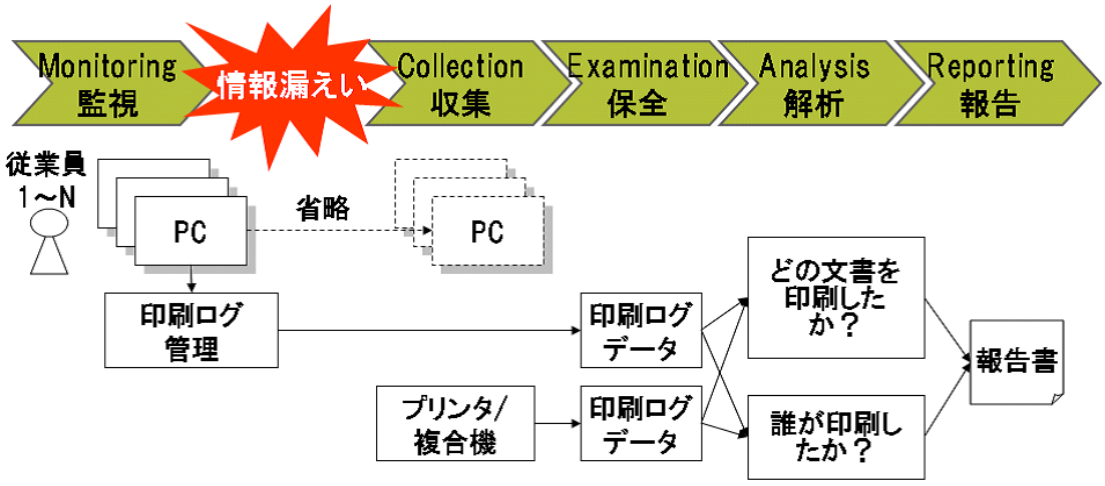

図 4.2: 拡張フォレンジックプロセスによる漏えい調査

このような Monitoring は，印刷以外の漏えい経路である，電子メール，外部媒体，Web に対しては，それぞれメールサーバ，Proxy サーバ，外部媒体書き出し管理サーバで日常的な業務での利用を監視することが既に広く行われている [108]．しかし，印刷に関しての Monitoring の研究はほとんど見当たらなかった．

拡張フォレンジックプロセスによる印刷の漏えい調査では，Monitoring で職員による印刷を常に監視し，その結果を印刷ログに記録し，集中管理を行う（図 4.2 中の印刷ログ管理）．そのため，情報漏えい発覚後に「いつ，誰が，何を印刷したか」を絞り込む Analysis を実施するために，物理的に PC を押収する Collection の工数は不要となる（図 4.2 中の点線で囲んだ PC）．更に Examination ではイベントログの回収やスプールファイルの復元などに取って代わり，扱いやすい印刷ログデータを扱う（図 4.2 中の印刷ログデータ）．なお，Reporting は従来のフォレンジックプロセスと共通である．

4.3.2 Monitoring フェーズの基本設計

オフィスにおいて印刷は広く使われるため，Monitoring 設計に関して次項に述べる工夫が必要となる．

監視内容

職員による印刷の事実を，事後の Analysis で導き出すために，従来の印刷に関するイベントログ [109] でも記録している「日付」「時刻」「印刷されたドキュメン

ト名」「プリンタ名」「ドキュメントのバイト数」「印刷したページ数」は最低記録すべき情報である．しかし，これだけの監視内容だけでは「何を印刷したか」については「印刷されたドキュメント名」しか残っていないため，本当にどのような内容が印刷されたのかを Analysis で調べることが困難となる．そこで，監視内容に関する要件を，次を満たすことと考えた．

- 印刷内容を目視確認できること
- 検索できること
- サイズが小さいこと

印刷監視により取得可能なデータに着目すると，表 4.2 に示すようにまず (1) スプールファイルがある．スプールファイルとは印刷時に必ず作成される一時データであり，RAW，EMF，XPS，PS の各形式がある．次にスプールファイルから変換した (2) 画像ファイルや，印刷時にプリンタドライバでテキスト情報だけを取得した (3) テキストファイルも挙げられる．

表 4.2: ログに記録する印刷内容の比較

比較項目	(1) スプールファイル	(2) 画像ファイル	(3) テキストファイル
印刷内容の目視確認	○（印刷内容そのものを確認可.）	○（印刷内容を画像で確認可.）	×（テキスト部分のみ確認可．図面，写真，レイアウトは欠落.）
検索性	×（EMF, XPS, PS ファイルはテキスト取得が可．RAW ファイルは不可.）	×（OCR を使ってテキスト取得可．ただし，OCR の読み取りミスあり.）	○（可能.）
サイズ	×（比較的大きい.）	×（大きい.）	○（小さい.）

スプールファイルは比較的ファイルサイズが大きく，スプールファイルの形式によっては検索に不向きな場合もある．また，画像ファイルの場合，大量のログから検索するには OCR (Optical Character Recognition) の利用によるテキスト検

索が一般的だが，OCR の読み取りミスを考慮しなければならない．更に，テキストファイルのみの記録の場合，サイズは小さい一方で，テキスト情報だけでは図面や写真，レイアウトが欠落してしまう．

そこで Monitoring フェーズで記録する印刷内容として，サイズを小さくしつつ必要な情報を欠落させないため，(2) 画像ファイルと (3) テキストファイルを併用する方針とした．なお文献 [110] によると，上記 (1) スプールファイル（RAW，EMF，XPS，PS 形式）は印刷元の電子ファイルに比べて平均 1.85 倍のサイズ，上記 (2) 画像ファイルと (3) テキストファイルを合わせたログサイズは印刷元に比べて平均 0.04 倍のサイズであることが知られており，上記方針によるとサイズを大きく削減できる．

監視場所

印刷を監視する場所の要件は，オフィスでの監視を考慮し，次を満たすことと考えた．

- 画像とテキストの両データを取得できること
- 既存環境からの移行が容易なこと

監視場所には，オフィスにおける印刷方法からして，表 4.3 に示すように (1) プリンタ/複合機，(2) プリントサーバ，(3) クライアント PC の 3 箇所が挙げられる．印刷はプリンタ/複合機を使って出力されるため，こうしたハードウェアでの監視は確実な反面，オフィスにある全てのプリンタ/複合機にて印刷監視機能を搭載するのは移行コストが高くなる．また，プリントサーバはスプールファイルを処理するため，画像データ及びテキストデータを取得可能な反面，既にプリントサーバを利用していたオフィスでは入れ替えが必要であり，また小規模オフィスなど今までプリントサーバが不要だったオフィスに導入するのに新たなコストがかかる．クライアント PC では，印刷は必ずプリンタドライバ経由で行われるため，プリンタドライバでの監視が可能であり，プリンタドライバの入れ替えだけで導入が可能となる．

そこで Monitoring フェーズでの監視場所は，既存環境からの移行の容易性を重視し，(3) クライアント PC での監視を行う方針とした．

表 4.3: 印刷監視場所の比較

比較項目	(1) プリンタ/複合機	(2) プリントサーバ	(3) クライアント PC
画像データとテキストデータの取得	○（スプールファイルからの変換で可. あるいは OCR を利用.）	○（スプールファイルからの変換で可. あるいは OCR を利用.）	○（プリンタドライバで可.）
既存環境からの移行	×（プリンタ/複合機の入れ替えが高価.）	×（プリントサーバの入れ替えや新規設置が必要.）	○（プリンタドライバの入れ替えだけで可.）

4.4 印刷監視システムの開発

4.4.1 システムアーキテクチャ

Monitoring フェーズで使用する印刷監視システムのアーキテクチャを図 4.3 に示す.

印刷監視システムは大きく「仮想プリンタドライバ」と「印刷ログ管理サーバ」とで構成する．仮想プリンタドライバは，各クライアント PC 上のプリンタドライバとして機能し，印刷を監視し，印刷ログを生成する．印刷ログは印刷ログ管理サーバに収集する．もし紙文書の情報漏えいが見つかった場合，調査員は漏えいした紙文書の特徴（テキスト，画像）を印刷ログのテキストデータや画像データと比較し，漏えいした紙文書と同じ印刷を，いつ，誰が，行ったのかを印刷ログ管理サーバに問い合わせて調べることができる．

4.4.2 仮想プリンタドライバ

仮想プリンタドライバは，印刷時に印刷内容として画像とテキストの両データを取得し，印刷ログを生成・送信する．画像データを取得するには印刷時に必ず作成されるスプールデータを変換すれば良い．また，印刷時にテキストデータを取得する方式として，文献 [111] によると，文字コード処理方式が知られている．文字コード処理方式は，OCR を使わずに文字情報を取得する方式であり，プリンタドライバでの印刷処理時に文字コード処理をフッキングすることで，印刷ページ

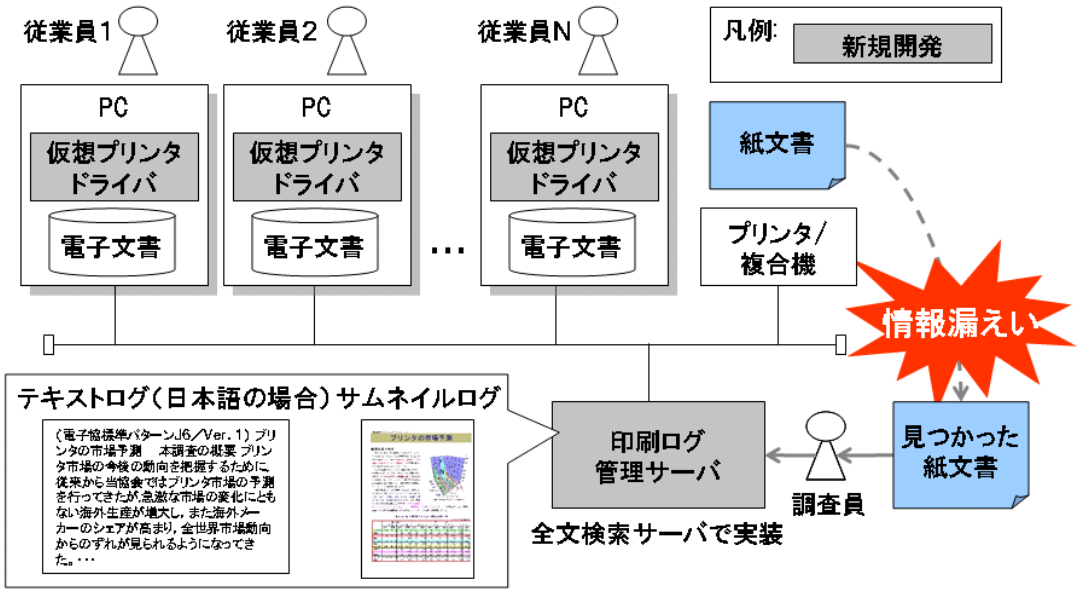

図 4.3: 印刷監視システムアーキテクチャ

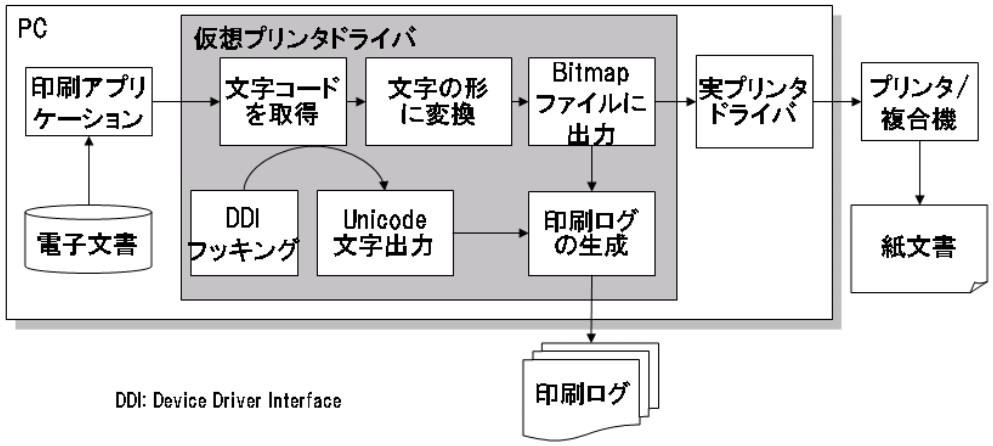

図 4.4: 仮想プリンタドライバのブロック図

のフルテキストを取得する．本方式は OCR に比べて高速かつ正確にテキストデータを取得可能である [111]．この文字コード処理方式を活用し，仮想プリンタドライバを設計した．仮想プリンタドライバは図 4.4 に示すように，通常印刷しつつ，ページ単位での画像データ取得とテキストデータ取得を同時に行う．

仮想プリンタドライバが動作する PC では，全ての PC に仮想プリンタドライバ

がインストールされることと，仮想プリンタドライバの置き換えや削除がなく正常に動作する環境であることが前提となる．仮想プリンタドライバがインストールされていないPCの検出には，ネットワークに接続されたPCにインストールされたソフトウェア一覧を監視するPC管理ツールの利用が有効である．また，仮想プリンタドライバの正常な動作環境を確保するために，仮想プリンタドライバの置き換えや削除を防止あるいは検出するには，PC起動時にTPM（Trusted Platform Module）を用いてソフトウェア構成を調べる方法 [112–114] が有効である．

4.4.3 印刷ログ管理サーバ

印刷ログ管理サーバは，図4.5に示すように，仮想プリンタドライバから生成される印刷ログを収集・蓄積し，印刷内容のテキスト部分をクロールしインデックス化を行う．また，調査員が漏えいした紙文書に関連する印刷ログを素早く見つけるために，検索インタフェースを設ける．検索インタフェースでは，絞り込み用の検索キーワード入力を受け付け，そのキーワードを含む印刷ログ（テキスト，画像）を表示する．

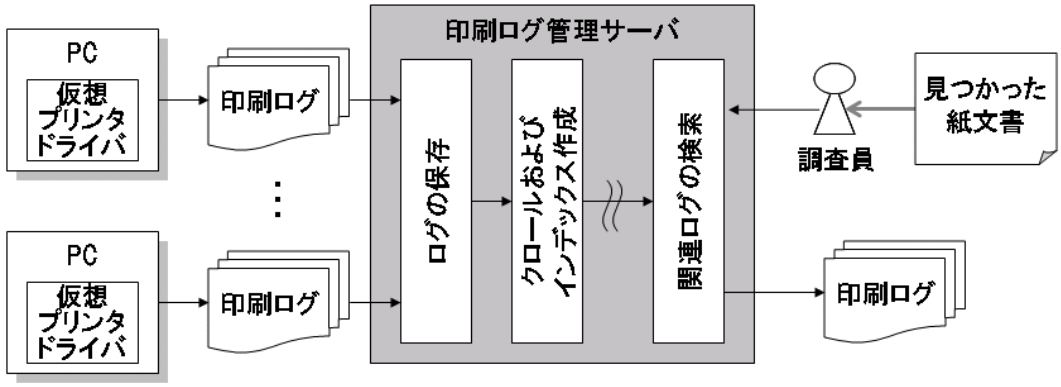

図 4.5: 印刷ログ管理サーバのブロック図

このような印刷ログ管理サーバのアーキテクチャは，近年，企業や組織での利用が増えている全文検索システムと類似している．そのため，実装にあたっては例えば企業向けの全文検索サーバ [115, 116] の利用が考えられる．

印刷ログ管理サーバでも，4.4.2項に述べたPCの場合と同様に全文検索に使用するプログラムの置き換えや削除がないことや，印刷ログの改ざんや削除がなく，正常に動作する環境であることが前提である．

4.4.4 印刷ログ形式

印刷ログには 4.3.2 項に述べたように従来のイベントログで記録していた項目に加え，印刷内容を記録する．この印刷内容について，4.4.2 項にてページ単位でのテキストと画像を印刷内容として生成することを述べた．また 4.4.3 項で述べたように，印刷ログ管理サーバでは，検索可能なテキスト部分と，画像部分とが容易にリンクできることが望ましい．

そこで印刷監視システムでは，印刷内容のテキスト部分については，印刷のページ単位毎に，次に示すファイル名で管理する．また印刷内容の画像部分については，拡張子を除いて同じファイル名とする．

＜日付・時刻＞_＜コンピュータ名＞_＜ユーザ名＞_＜プリンタ名＞_＜印刷されたドキュメント名＞_＜ドキュメントのバイト数＞_＜印刷したページ数＞_＜印刷内容の総ページ数＞_＜印刷内容のページ番号＞.txt

印刷ログ形式を上記とすることで，印刷ログ管理サーバが行うクロール時に，印刷のページ単位で区切ってインデックス化を行う．また検索結果の表示時にも，印刷ログのファイル名から「いつ，誰が，何を印刷したか」が一目瞭然であると共に，印刷ページ数が多い場合にも何ページ目であるかが容易に判明する．更に検索結果ではファイル名の拡張子を変えるだけで，画像ファイルとのリンクも容易である．

4.5 印刷フォレンジック調査の効率性の評価

4.5.1 情報漏えいのシナリオ

情報漏えい調査は，置かれた状況や調査目標などが個々の事件によって，大きく異なることが多い．そこで印刷フォレンジック調査が必要となる状況を明確化するため，次に示す漏えい事件を想定する．

(1) ある組織のプロファイル
ある組織で働く職員は，国家機密（例えば国際テロ捜査情報など）に該当する文書を作成し処理する．セキュリティ管理者は，厳格なセキュリティポリシーを職員に課しており，年に一度の割合で職員の作業記録を監査する．

(2) 情報漏えい事件の発覚
ある日，書店で売られている書籍に，国家機密に関する特定の文書が掲載されているとの連絡が入った．調査員が該当する書籍を調べたところ，その国家機密は約 1 年前に作成されたものであり，特徴的な印刷フォントの形

からして，組織内で使われるワープロソフトで作られた電子文書が，組織内の特定のプリンタから印刷された紙文書であって，その紙文書がスキャンされた形で書籍に含まれることが判明した．

(3) フォレンジック調査の目的
調査員は，組織で作られた文書のうち，どの電子文書が印刷されたのか，誰がそれを印刷したのかを調べるよう命じられた．1 週間以内に第一次報告，1ヶ月以内に最終報告を行う必要がある．もしこれらの事実が判明すれば，ある組織は適切な法的処置に訴える予定である．

なお，具体的な作業量を求めるために，以下に示す前提条件を設けた．

- 国家機密を扱う職員は，特定の部署に限定される．ここでは 30 名とする．
- 前記部署では一人が一台の PC を使い業務を行う．PC の HDD 容量は平均 40GByte である．
- 部署で一台のプリンタを共有する．
- 職員は一人で当たり 1 年で平均 3,000 枚の印刷を行う．業務日数を 200 日として 1 日で平均 15 枚の印刷を行う．
- 前記部署では改変が許されないフォントを使って印刷を行う必要があり，印刷時に付加情報（印刷者 ID など）を印刷物に埋め込む電子透かし [117–119] はフォントの改変にあたる可能性を否定できないため，電子透かしは使っていない．

つまり特定の部署で印刷された約 90,000 枚の中から，情報漏えいにつながった形跡を絞り込むことがフォレンジック調査の作業となる．調査員はまず 1 週間以内に第一次報告を行うのに必要な人数の見積もりを行う方針とした．

4.5.2 従来のフォレンジックプロセスの作業工数

比較のため，従来のフォレンジック調査，つまり 4.2.2 項で述べたような PC 押収，HDD データコピー，専用ツールによる解析，報告というプロセスの作業工数を見積もると，次に示すとおりとなる．

(1)Collection
PC を押収し，その HDD データの完全コピーを行う．単なるコピーではなく

完全コピーを行うことで，一時的に作成されたスプールファイルまで復元する．フォレンジック専門業者 [120] によると，40GByte の HDD で 4 時間以上の工数がかかるといわれている．30 台ではのべ 120 時間の作業量となる．完全コピーしたデータ量は 1.2TByte に及ぶ．

(2)Examination

完全コピーしたデータを，専用フォレンジックツール [106, 107] で読み込ませ，事前解析処理（削除ファイルの復元，ファイルのハッシュ値計算，インデックス化など）を行う．専用フォレンジックツールのパフォーマンステスト結果 [121] によると，市販で購入可能な高性能マシンで，120GByte の HDD の事前解析処理に 5.32 時間を要すると述べられている．よって，データ量が 1.2TByte の場合には 53.2 時間を要する．

(3)Analysis

調査員は専用フォレンジックツールを使って，漏えいした紙文書を印刷した痕跡を調べる．いくつかの調査手法を組み合わせ,「いつ，誰が，何を印刷したか」の情報を引き出していく．

- レジストリを対象に，特定のプリンタを使用していたかどうか
- スプールファイルを対象に，漏えい文書を印刷したかどうか
- イベントログを対象に，漏えい文書と同じドキュメント名の印刷がないかどうか
- 電子文書を対象に，漏えい文書と同じファイルを保持していたかどうか，当該ファイルにいつアクセスしたか

前記 Examination で行った事前解析処理をしておけば，特定のワープロファイルの形式のみのフィルタリングや，ある日時以降に作成されたファイルのフィルタリングや，当該ファイルに含まれる文字列を高速に全文検索することが可能である．こうした Analysis に要する時間は，職員一人当たり約 1 時間として 30 名で約 30 時間を要すると考えられる．

以上の (1)〜(3) からすると，従来のフォレンジックプロセスではのべ約 200 時間にも及ぶ作業量となる．調査員 1 名当たり 1 日に 10 時間作業したとしても，1 週間（5 業務日）以内に第一次報告を行うためには，約 4 名の調査員が必要となる．もし組織内で上記人数だけの調査員を確保できないようであれば，フォレンジック専門業者へ委託することを検討しなければならない．

4.5.3　拡張フォレンジックプロセスの作業工数

提案した印刷監視システムを利用することで，提案型のフォレンジック調査の作業工数は，次に示すとおりとなる．ここで仮想プリンタドライバはドライバ開発キット [122] を使って開発し，また印刷ログ管理サーバは，オープンソースの全文検索サーバ [116] を利用して構築した．

(1)Monitoring
印刷監視システムを利用することで，職員には新たに 2 つの負荷がかかる．

- 仮想プリンタドライバのインストール
- 印刷ログの一時保管とネットワーク転送

プリンタドライバのインストールは，通常のオフィスでプリンタ/複合機を使いはじめる場合には，必ず発生する作業である．そのため仮想プリンタドライバをインストールする負荷は，追加の作業とはならない．

また印刷ログのサイズを実測するため，プリンタ用標準テストパターン [123] を仮想プリンタドライバで印刷し，印刷ログ（テキスト，画像）を生成した．なお画像データとしては，様々なサイズで取得することが考えられるが，ここでは印刷スプールファイルの一種である XPS ファイル [124] のサムネイル画像と同じサイズで取得し実測した．その結果，1 ページ当たり平均 17.6KByte（テキスト 2.0KByte，画像 15.6KByte）であった．よって 1 日当たりの印刷ログは平均 264KByte である．本サイズであれば，印刷ログの PC 上での一時保管とネットワーク転送にはほとんど負荷はかからないと考えられる．

また印刷ログは 1 年間で 1.58GByte となる．そのうちテキスト部分は 180MByte 相当である．本テキスト部分を対象にインデックスを印刷ログ管理サーバで作成したところ，インデックスサイズは 753MByte であった．

(2)Collection
印刷監視システムにより印刷ログが記録及び回収されているため，あらためて PC を押収する必要はなくなる．作業工数はゼロである．

(3)Examination
同様に作業工数はゼロである．

(4)Analysis
調査員は，漏えいした紙文書に含まれる特徴的なキーワード（「機密　報告書」など）を，印刷ログ管理サーバの検索インタフェースを使って検索する．

90,000 件の印刷ログを対象に 1 度の検索に要する時間を，全文検索サーバの検索ログに含まれる応答時間で確認したところ，平均 0.67 秒であった．全文検索は 1 度の検索では漏れやノイズが入ることから，繰り返し検索することが通常である．その場合にも，前記実測値からすると 1 時間程度で済むと考えられる．従来のフォレンジックプロセスの Examination で行っていた事前解析処理に相当する時間のかかる処理を，提案方式では日常的に，例えば深夜などの空いた時間に行うことで，漏えい発覚時には Analysis から着手できる点で優れている．

以上の (1)〜(4) からすると，拡張フォレンジックプロセスでは，漏えい発覚後の調査の作業量が 1 時間程度で済む．よって 1 週間以内に第一次報告を行うためには，調査員は 1 名でも十分に対応可能である．

4.5.4 考察

作業工数の削減量

印刷監視システムを使った拡張フォレンジックプロセスでの作業工数は，表 4.4 にまとめたように，従来約 4 名の調査員が必要となるのに比べて，提案方式ではほぼ 1 名の調査員だけで済み，大きく削減が見込めることが判明した．フェーズ別の工数の点から見ると，Collection と Examination で必要だった作業時間が削減されたことが大きい．つまり提案方式は，4.2.3 項で述べた課題である PC 押収工数を大幅に削減できる点で有用である．また，作業途中で発生するデータ量に着目すると，従来のフォレンジックプロセスでは最大で 1.2TByte のデータを扱うのに対し，拡張フォレンジックプロセスでは最大 2.3GByte のデータで済む．そのため，フォレンジック調査の途中で必要となるストレージリソースも数百分の 1 程度で済む．

職員数が増えた場合の影響

本シナリオでは調査対象とする職員数を 30 名として比較したが，実際の情報漏えい事故ではもっと多数の職員が疑われる可能性がある．従来のフォレンジックプロセスでは，職員一人当たりの調査に約 6.7 時間を要し，職員数が増えるほど調査に要する時間も比例して増加する．一方，拡張フォレンジックプロセスでは，Monitoring での印刷ログやインデックスのサイズは職員数に比例して増えるものの，印刷ログ管理サーバとして活用した全文検索サーバ [116] では，約 2 億文書の検索が可能といわれており，そのため職員数 6,000 名程度の規模までなら同程度のレスポンスを保持しつつ，拡張可能であると考えられる．

表 4.4: フォレンジック調査の作業工数の比較

フェーズ	従来のフォレンジックプロセス	拡張フォレンジックプロセス
Monitoring	なし	印刷ログ：1.58GByte/年, インデックス：0.75GByte/年
Collection	コピー工数：120 時間 コピー量：1.2TByte	なし
Examination	事前解析：53.2 時間	なし
Analysis	約 30 時間	約 1 時間
調査時間の合計	のべ約 200 時間	のべ約 1 時間
必要な人数の見積もり	約 4 名で 1 週間	1 名で 1 週間未満

印刷からの漏えいに対する抑止効果

拡張フォレンジックプロセスは，調査工数を削減する上で有効である．その一方で，実際に法的手段に訴えるとした場合に，印刷監視システムで絞り込まれた「いつ，誰が，何を印刷したか」の情報の証拠性が疑われる可能性がある．なぜなら印刷監視システム自身の動作の完全性や，記録した印刷ログの真正性や完全性まで問われるためである．こうした法的手段まで見据えた場合には，最初に印刷監視システムで疑わしい人物を早期に絞り込み，その後に時間をかけて従来のフォレンジックプロセスを適用することで証拠性の高い情報を引き出すという併用策が考えられる．いきなり従来のフォレンジックプロセスを適用する場合に比べて，絞り込みの効率化と法的手段への訴えを両立できる．このため，漏えい抑止効果を高めることができる．

また，印刷監視システムを運用するためには，印刷ログ管理サーバという新たなサーバをオフィスに設ける必要がある．情報漏えいという有事の際にだけ使うサーバとして見た場合には，投資対効果が低い．そこで有事に限らず平時においても，印刷監視システムを定期的な監査で不審な印刷がないかの発見にも使うことで，オフィスの職員に対する抑止効果を更に高めることにも役立つ．

4.6 関連研究

情報セキュリティの研究の中でも，紙文書や印刷に関わる研究は多くは見当たらない．また，OS が持つ印刷セキュリティ機能についても，OS が次々にバージョンアップしてきたのに対して，本稿で述べたような機能は見当たらない．ここでは，印刷からの情報漏えいを防止することを目的とする関連研究を述べる．

Monitoring（印刷の監視）

本稿で述べた Monitoring に関連する研究は，広く紙文書のセキュリティ対策を整理した文献 [125] や，印刷履歴を取得する印刷管理サーバ製品 [126, 127] で見られる．印刷管理サーバ製品では，プリントサーバ上で印刷ジョブからテキスト情報を取得し，印刷ログとして記録する．また別の研究 [128] では，EMF スプールファイルからテキスト情報を取得する．本稿で述べた仮想プリンタドライバ方式による印刷履歴取得は見当たらない．本方式は 4.3.2 項で述べたように，既存環境からの移行が容易な点で有利である．

電子透かし

漏えい防止のため，電子透かし技術を使った印刷の研究 [117] や製品 [118, 119] が知られている．電子透かしにより，印刷時に付加情報（印刷者 ID など）を印刷物に埋め込む．もし紙文書の漏えいが見つかったときには，前記付加情報を目視あるいはスキャンなどによって抽出することで，調査員は付加情報を確認できる．電子透かしは情報漏えいの発覚後のみに有用である．一方，本稿で述べた印刷監視システムは，4.5.4 項で述べたように，漏えい後に限らず平時の定期的な監査にも有用である．

4.7 おわりに

オフィスからの情報漏えい経路のうち紙文書（印刷）に注目し，印刷フォレンジック調査を効率化するため，新たな拡張フォレンジックプロセスを提案した．また前記プロセスを実現するために，印刷監視システムを設計・開発した．評価の結果，従来のフォレンジックプロセスでは 1 週間以内に一次報告を行うために約 4 名の調査員が必要だったのに対し，提案方式によると 1 名で対応可能な見通しを得た．提案方式によって日常的に職員に増える負荷も小さい見込みを得た．

今後の課題は，実フィールドでの情報漏えい調査時に，印刷監視システムの有効性を検証することである．

第5章　不正プログラムから情報資産を保護するクライアント向けファイルアクセス制御方式の開発

5.1　はじめに

コンピュータのネットワーク化が急速に進み社会基盤を担う一方で，コンピュータがウイルス・ワームに感染することは深刻な問題となっている．とくに近年ではウイルス・ワームの感染経路が多様化し急速に感染拡大する傾向があり，ウイルス・ワームの感染はコンピュータの管理者から利用者にいたるまで幅広い者にとって懸念事項となっている．例えば，警察庁が民間企業・各種団体を対象に行った情報セキュリティ対策の実態調査 [12] によると，過去 1 年間に発生したセキュリティ問題のうちウイルス・ワーム感染が圧倒的に多いと報告されており，今後も継続してウイルス・ワーム対策を強化していくことが重要となる．

ウイルス・ワームに感染した時の被害は多岐に渡り [129,130]，システムが起動できなくなることやネットワークトラフィックを著しく増大させるといった可用性の損失をはじめ，ウイルスが機密データを第三者に流出する機密性の損失や，利用者が知らないうちにウイルスがデータを操作するといった完全性の損失まで広範囲となる．被害額の点からすると 2003 年の国内のウイルス被害総額は 3,025 億円と推計され [131]，とくに機密性が損失した場合の被害はたとえ一回でも甚大なものとなる．

一方，これまでクライアント・サーバ型により発展してきた企業のコンピュータネットワークにおいて，情報資産がサーバ側にあることは周知の通りであるが，実際にはクライアント側にも多くの情報資産が存在する．例えば文献 [132] によると企業における情報資産の約 6 割がクライアントに保護されないまま存在すると指摘されており，先に述べたウイルス・ワーム感染時の機密性や完全性の損失は，サーバよりもクライアントの方がより深刻な問題となっている．

情報資産はコンピュータ上でファイルという形式で存在する．クライアントにあるファイルとは，システムファイル，プログラムファイル，ユーザデータファイルに大きく分類できる．システムファイルやプログラムファイルはたとえ改ざんされてもインストール CD から復旧することができ，また漏えいの対象にはまずなり得ない．一方ユーザデータファイルは，具体的にはクライアントで利用者が自ら作成したファイルや，サーバからダウンロードしたファイルなどが相当する．例えば企業でいうユーザデータファイルは報告書や提案書や顧客情報などのデータを格納し，さらには動画や音声といったデータも格納することが予想される．これらのユーザデータファイルにこそ機密データや重要データが含まれる．過去にこのようなユーザデータファイルを狙うウイルスもいくつか確認されており [133]，今後はウイルス・ワームがユーザデータファイルを狙うことが増加することも推測される．よってユーザデータファイル自体をウイルス・ワームから保護することはますます重要性を増す．

本章は以上のことから，クライアント上のユーザデータファイルを，ウイルス・ワームをはじめトロイの木馬といった不正プログラムから保護することを目的とした，クライアント向けのファイルアクセス制御方式を提案する．本稿で述べるファイルアクセス制御方式とは，筆者らがこれまでサーバ向けに開発してきた耐侵入型アクセス制御 [134,135] をクライアントに応用したものであり，一般利用者でも容易に使えるようにした次に示す特長をもつ．

- 多用途なクライアントに対して，正常アクセスの分析から多様なアクセスが代表的なパターンに分類できることを特定し，
- 上記正常アクセスを，OS の持つ構成情報を参照して準自動的にポリシー設定するようにした
- ポリシー設定後の修正を，利用者が対話式な操作で実施できるようにした

以下，5.2 節で一般的なクライアント向けのセキュリティ対策を，5.3 節で耐侵入型アクセス制御をクライアントに適用する上での課題を述べる．5.4 節で課題を解決するためのクライアント向けファイルアクセス制御方式を提案し，5.5 節で試作開発結果とその考察を述べる．

5.2 不正プログラムからユーザデータファイルを保護するセキュリティ対策

本節ではまず，クライアントに侵入する不正プログラムからユーザデータファイルを保護する従来のセキュリティ対策を全般的に述べる．

5.2.1 クライアント向けセキュリティ対策の現状

不正プログラムからユーザデータファイルを保護するには，まずは不正プログラム自体のクライアントへの侵入を防ぐことが第一である．一般的に実施される対策には，次のものが挙げられる．

- アンチウイルスソフトの導入
- OS セキュリティパッチをはじめとする各種パッチの適用
- パーソナル・ファイアウォール（FW）の導入

しかし，感染経路が多様化し急速に感染拡大するウイルス・ワームに対してワクチンの更新や最新パッチの適用が間に合わず，ウイルス・ワームに対してクライアントが無防備になるという時間帯が存在する．さらに，パーソナル FW では利用者が安易なダウンロードを実施したときにトロイの木馬が侵入してくる場合には対応できない．よって，仮に不正プログラムがクライアントに侵入したとしても被害を防ぐ事後防止策も重要となる．こうした事後防止策には，次のものが挙げられる

- 制限付きアカウントの使用
- バックアップの実施

ここで制限付きアカウントの使用とは，利用者が通常は制限付きアカウントを使用し必要なときだけ OS 管理者権限を使用することで不正プログラムが侵入した場合にもコンピュータ全体に被害が及ぶことを防ぐものである．しかし，制限付きアカウントで読み書きするようなユーザデータファイルに対しては改ざん・漏えいの被害が及んでしまう．また，バックアップの実施では，バックアップを取るまでにユーザデータファイルを改ざんされた場合には復旧もできず，漏えいには無効である．よって，これらの事後対策をさらに補完できるような，ユーザデータファイルを直接的かつリアルタイムに保護できる対策が望まれ，この対策を実現する手段としてファイルアクセス制御が考えられる．

5.2.2 従来のファイルアクセス制御と耐侵入型アクセス制御

ユーザデータファイルを保護するファイルアクセス制御は，クライアントに適用することを考慮すると次の要件を満たすべきだと考える．

要件１ 専門知識をもたない者でも，手間をかけずに容易にアクセス制御の設定を行えること

要件２ これまで作成・蓄積したユーザデータファイルを継承して利用できること

一般にファイルアクセス制御と言えば，汎用 OS 付属のファイルシステムの多くが有する「任意アクセス制御」と，軍事向けなど高度なセキュリティを要する場合に利用される Trusted OS のもつ「必須アクセス制御」が挙げられる [13]．しかしこれらのファイルアクセス制御には以下のような問題がある．

まず「任意アクセス制御」は，ファイルの所有者がファイルへのアクセス権（ファイルを共有可能とする範囲）を指定できるものである．しかし，5.2.1 項で制限付きアカウントを使用するときの現状でも述べたように，ユーザ A の権限で不正プログラムが動作した場合，ユーザ A にアクセス権が与えられたファイルは全て無防備となる．よって不正プログラムからユーザデータファイルを保護することができない．

また「必須アクセス制御」とは，取り扱い資格を与えられていないサブジェクト（ユーザやプログラムなど）は，機密性の高いオブジェクト（ファイルやデバイスなど）へのアクセスを制限されるものである．かりに不正プログラムが混入したとしてもユーザデータファイルへの被害を極小化することができる．しかしそもそも Trusted OS を運用する時にサブジェクトとオブジェクトの対応関係を設定すること自体が難しく運用負荷が高いと指摘されている [136]．一方でこうした運用負荷の高い必須アクセス制御のポリシー設定を簡易化するアプローチもある [77, 137–139]．これらは記述の複雑なポリシーを直接編集するのではなく理解を容易にする中間言語を利用して設定簡易化する方式 [137–139] と，実際にプログラムやサービスを走行させて発生したアクセス履歴をもとに設定簡易化する方式 [77] である．しかし前者の中間言語を利用する簡易化方式では中間言語を理解することが前提であることから専門知識が必要となる．また後者のアクセス履歴をもとにした簡易化方式では多用途なクライアントに適用するにはますます手間がかかってしまう．よって前記（要件１）を満たせない．またこれまで汎用 OS で作成・蓄積されることの多いユーザデータファイルは，アプリケーションの数の少ない Trusted OS では継承して利用することが難しくなり前記（要件２）も満たせない．

以上述べた任意アクセス制御と必須アクセス制御とは異なるものとして，筆者らはこれまでに「耐侵入型アクセス制御」と呼ぶファイルアクセス制御を開発してきた [134, 135]．耐侵入型アクセス制御は主にインターネットサーバへの適用を対象としたものであり，図 5.1 に示すようにファイルにアクセス可能なプログラムを制限できる．また汎用 OS にアドオン可能である．このため業務で利用するプロ

グラムにあらかじめ限定しておけばユーザデータファイルを不正プログラムから保護することができる．このようなアクセス制御を決めるポリシー設定は，後述する 5.3.1 項で述べるように分かりやすい．またアプリケーションを継承利用できるため前記（要件２）を満たす．よって筆者らはユーザデータファイルを保護するために耐侵入型アクセス制御を採用した．本稿では以下，前記（要件１）を満たすことを目標としたポリシー設定の簡易化について述べる．

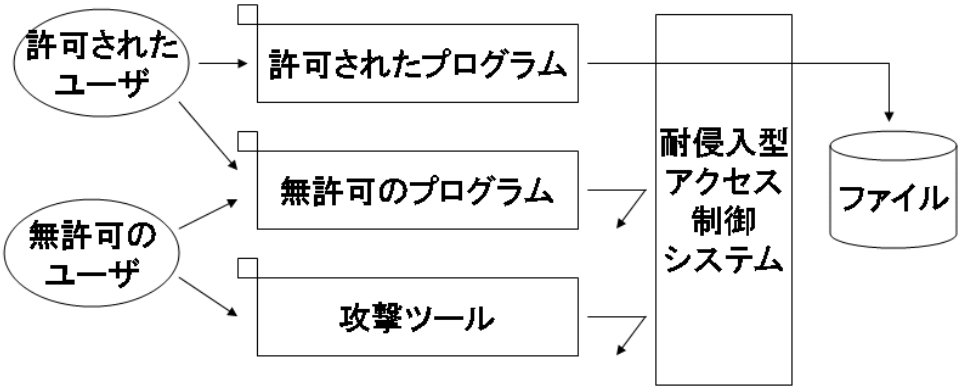

図 5.1: 耐侵入型アクセス制御システムの概要

5.3 耐侵入型アクセス制御をクライアントに適用する上での課題

5.3.1 サーバ向けの耐侵入型アクセス制御

耐侵入型アクセス制御ではホワイトリスト型のポリシーをもとに，ファイルアクセスの制御を行う．つまり，あらかじめポリシーで許可しておいたアクセスだけを通し，それ以外のアクセスを禁止するというものである．例えば，電子商取引の Web サーバに耐侵入型アクセス制御システムを適用する場合，図 5.2 に示すポリシー例のように，サービス提供に必要最小限となる次のような正常アクセスだけを許可するよう各種パラメータを設定する．

1. カタログ情報のファイル（catalog.htm）には，Web サーバのプロセス（httpd.exe）だけが読み込み可となるよう各種パラメータを設定する．

オブジェクト	ユーザ	プログラム	特徴値	アクセスタイプ
C:¥www¥catalog.htm	www	C:¥prog¥httpd.exe	0x1234	Read
C:¥www¥customers.txt	www	C:¥prog¥register.exe	0xabcd	Read,Write

図 5.2: サーバ向けのアクセス制御ポリシーの例

2. 顧客情報のファイル（customers.txt）には，特定のCGIプロセス（register.exe）だけが読み書き可となるよう各種パラメータを設定する．

ここで図5.2に示すポリシー例の中でのパラメータの一つである特徴値とは，プログラムの真正性を確認するための情報（例えば，プログラムのサイズやハッシュ値）を登録したものである．図5.2に示すポリシーを設定したWebサーバ上では，保護対象オブジェクトに未許可のプログラムがアクセスしようとしてもブロックされ，さらに不正なプログラムが許可プログラムになりすましてアクセスしようとしてもブロックされる．一般にサーバは用途が限定的であり正常アクセスを特定しやすいため，サーバ向けにホワイトリスト型のポリシーを設定することは容易となる．

5.3.2 課題

5.3.1項で述べた耐侵入型アクセス制御をクライアントにも適用し，ユーザデータファイルを不正プログラムから保護しようとする場合，サーバに適用する時には問題にならなかったクライアント固有の課題が出てくる．

まずサーバ向けの場合にはサーバの用途が限定されるため，5.3.1項で述べたようにサービス提供に必要な正常アクセスを把握しポリシーを決めることが容易である．しかし，クライアントは多用途でありインストールされるプログラムも多様であるため，クライアント向けのホワイトリスト型ポリシーを決めるのに必要となる正常アクセスの把握が困難となる．

つぎにポリシーの初期設定は，サーバ・クライアントに関係なく耐侵入型アクセス制御を導入するときに必要な操作となる．しかし，クライアントの利用者はサーバの管理者に比べて十分に訓練されているとは限らず，例えばはじめてポリシー設定を行うような場合には何を設定すれば良いか分からないこともあり得る．それゆえポリシーを初期設定するための前提条件に，専門的な知識を求めることができない．またクライアントにインストールされるアプリケーションは一台ず

つ異なることが多く個別設定が必要となるため，ポリシーを初期設定することは煩雑な作業となる．さらに一度設定したポリシーを修正するには，修正対象箇所を特定し適切なパラメータに変更するという手間がかかる．アプリケーションの追加や更新が頻繁に起こりうるクライアントでは，追加や更新のたびにパラメータの変更を余儀なくされ，このようなポリシー修正の手間は利用者にとっての負担となる．

以上をまとめると，耐侵入型アクセス制御をクライアントに適用する上での課題は次のとおりとなる．

課題１ クライアント向けのホワイトリスト型ポリシーを決めるのに必要な正常アクセスの把握が困難なこと

課題２ 専門的な知識や煩雑な手間を必要とせずにポリシーを設定および修正できること

5.4 クライアント向けファイルアクセス制御方式の提案

本節では，5.3 節で述べたクライアントに適用する上での課題を解決した，クライアント向けのファイルアクセス制御方式を提案する．5.3 節で述べた（課題１）に対して下記（解決策１）で,（課題２）に対して下記（解決策２）（解決策３）で解決することにした．

解決策１ 正常アクセスの分析によるクライアント向けホワイトリスト型ポリシーの決定

解決策２ OS の持つ構成情報を参照した準自動的なポリシー設定

解決策３ 対話式によるポリシー修正

次項よりそれぞれの解決策について具体的に説明する．

5.4.1 解決策１：正常アクセスの分析によるクライアント向けホワイトリスト型ポリシーの決定

（課題１）に対してまず，クライアントで業務を遂行するのに必要なアクセス（以下，正常アクセスと称す）をサンプル収集し，次に収集した正常アクセスの分析を行うこととした．クライアントで想定される利用プログラムとその処理の一覧を表 5.1 に示す．

表 5.1: クライアントで想定される利用プログラムとその処理

利用プログラム	プログラムの処理
OS	起動，終了，ログイン，セキュリティパッチ適用
管理ツール	ユーザ設定，ディスク設定，ほか各種設定
エクスプローラ	コピー，移動，削除，名称変更，アクセス権変更，ゴミ箱を空にする，ゴミ箱から元に戻す
ウィルス対策ソフト	ファイルをスキャンする，パターンファイルを更新する
バックアップ	バックアップする，復元する
アーカイブソフト	圧縮，解凍
ネットワーク共有	リモートマシンからのファイルアクセス，各種ファイル操作
Web ブラウザ	ページ参照，各種設定変更，ダウンロード・アップロード
電子メール	メール送信・メール受信，添付ファイルの保存，メールへの添付，アドレス帳のインポート・エクスポート
ビジネスソフト（ワープロ，表計算，プレゼンテーション）	文書作成，編集，保存，印刷，OLE オブジェクトの埋め込み・リンク，Web ページとして保存

前記収集した正常アクセスをもとにホワイトリスト型ポリシーを設定することも一つの方法（前記文献 [77]）である．しかし，利用頻度が低いアプリケーションからのアクセスなど収集し忘れた正常アクセスがある場合には，不完全なホワイトリスト型ポリシーとなってしまう．そのためクライアントに導入する度に正常アクセスを収集しなくても済むように，前記収集した正常アクセスを何らかの着眼点からパターン化できないかと考えた．その結果，ユーザデータファイルに対する正常アクセスを図 5.3 に示す 3 パターンにほぼ分類できることが判明した．

1. 関連付けアプリケーション（AP）からのファイルアクセス（図 5.3 の (1)）
   ユーザデータファイルであればほとんどの場合，特定の AP と関連付けられているという点に着目した．ここで関連付け AP とは，ファイルに対するアクセス手段として利用される頻度の高いプログラムと言っても良い．例えばワープロファイルの場合，それに関連付けされたワープロソフトからのファイルアクセスが発生する．表計算ファイルには表計算ソフトからのファイル

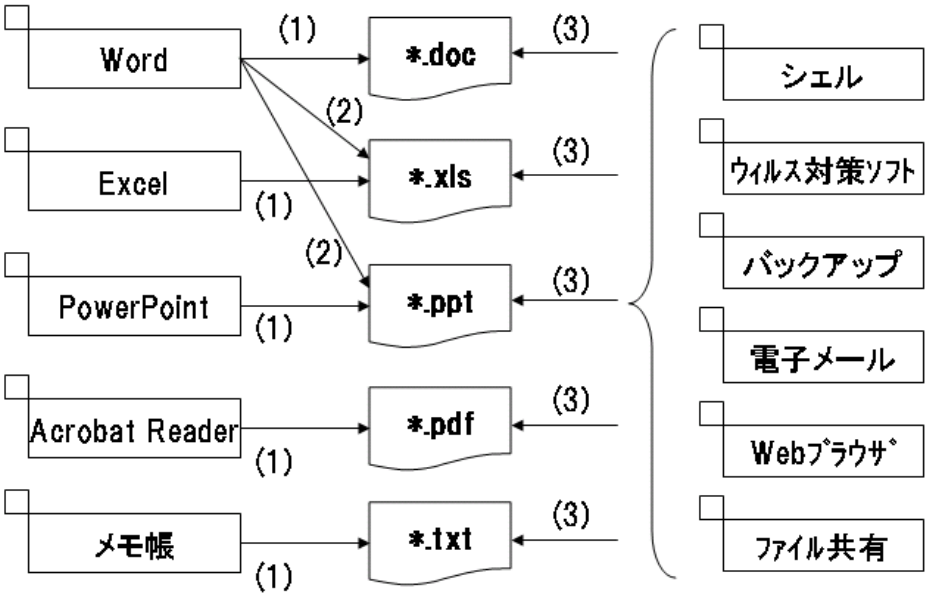

図 5.3: ユーザデータファイルに対するファイルアクセス

アクセスが発生する．

2. OLE 対応の AP からのファイルアクセス（図 5.3 の (2)）
   次に前記関連付け AP からは，関連付けされたファイル以外に対してもアクセスが発生する点に着目した．例えばワープロソフトは，表計算ファイルで作成したグラフオブジェクトをワープロファイルに埋め込むために，表計算ファイルにアクセスする．このようなある AP のデータを別の AP のデータ内部に取り込む技術は Windows OS では OLE と呼ばれる．関連付けされたファイルには，関連付け AP 以外にも OLE に対応した AP からのアクセスが発生する．

3. 用途別プログラムからのファイルアクセス（図 5.3 の (3)）
   さらに前記（１）（２）は主にユーザデータファイルの作成・編集という傾向が強いのに対して，そうした用途とは全く異なる用途で利用するプログラムからのアクセスもある点に着目した．こうした特定用途のプログラムは表 5.2 に示すように数を絞り込むことができるものとなる．この用途別プログラムからはあらゆるユーザデータファイルへのアクセスが発生する．

以上のパターン化によりユーザデータファイルへの多様な正常アクセスをまとめて把握できるようになる．よって，上記パターンの全てを許可することを，ク

表 5.2: 用途別プログラムの例

用途	プログラム例
ファイル操作	シェル，圧縮・解凍ツール
セキュリティ	ウィルス対策ソフト，バックアップツールファイル暗号化ソフト
ネットワーク	電子メール，Web ブラウザ，ファイル共有，リモートデスクトップツール

ライアント向けのホワイトリスト型ポリシーとして決定した．なお，上記パターンに分類されない正常アクセスがあったとしても後から容易にポリシーに追加可能であることを 5.4.3 項で述べる．

5.4.2 解決策２：OS の持つ構成情報を参照した準自動的なポリシー設定

上記（解決策１）で述べたパターン化されたものの中には，レジストリといった OS の持つ構成情報を調べることで，ファイルアクセスの内容を具体的に知ることができるものがある．そこで（解決策２）では，ポリシーの初期設定時に OS の持つ構成情報を参照することで下記に示すようにポリシー原案を自動的に生成することにした．その後は利用者がポリシー原案を編集することで設定を完了できるようにする．

解決策 2a 関連付け AP と OLE 対応の AP からのファイルアクセスは，例えば Windows OS ではレジストリに保持される情報から分かる [140]．ファイルの種類とそれにアクセスするプログラムを調べ，それらのファイルアクセスだけを許可するポリシー原案を自動生成する．

解決策 2b 用途別プログラムからは全てのファイルの種類へのアクセスを許可するよう，ポリシーを自動生成する．このような用途別プログラムのうち OS 標準で提供されるものならば，事前に分かる OS 標準の用途別プログラムをポリシー自動生成時に登録する．

解決策 2c OS 標準でない用途別プログラムは，利用者がクライアントを使い始めてからインストールしたものであると考えられる．OS 標準でない用途別プ

ログラムは，インストールされたアプリケーションの中から利用者が選択できるようにする．

以上のような準自動設定とすることで（課題２）に挙げた専門的な知識や煩雑な手間を低減できる．

5.4.3　解決策３：対話式によるポリシー修正

ポリシーを初期設定した後に

- アプリケーションが追加や更新された場合，
- ユーザデータファイルへのアクセスが必要にも関わらず，前記（解決策２）で自動生成されるポリシーではアクセス許可されない場合，

それらのアプリケーションはポリシーで許可されていないためにユーザデータファイルにアクセスできない．前記の（課題２）で述べたように，こうしたアプリケーションをポリシーで許可するには，5.3.1 項で述べたポリシーに対してパラメータの変更対象箇所を探す手間などが必要となり，利用者にとって手間がかかる．（解決策３）では，必要なアクセスを許可したい場合に利用者が対話式にポリシーを修正できるようにする．これにより利用者は変更対象箇所を探す手間をかけずにパラメータを変更することができる．

5.5　クライアント向けのポリシー設定支援ツールの開発

本節では，5.4 節で述べた方式にもとづき試作したクライアント向けのポリシー設定支援ツールについて述べる．

5.5.1　利用者に要求する前提知識

前述の（解決策２）ポリシー原案の自動生成によりファイルとプログラムとの対応関係といった専門的な知識はほぼ不要となるが，その一方で自動生成されたポリシー原案の編集のためにはツールの利用者にも多少の知識が必要となる．こうした編集時における前提知識も少なくて済むように，ポリシー設定支援ツールの開発にあたり，利用者が最低限次に示す前提知識を持っていれば原案を編集できるようにツールを設計した．

- ユーザデータファイルを置くフォルダの絶対パスを知っていること

- 重要データや機密データを格納するファイルの種類（拡張子）を知っていること
- クライアントに何のアプリケーションをインストールしたかを名称で知っていること

5.5.2 システム構成

クライアントとして Windows 2000/XP を対象にポリシー設定支援ツールを試作した．図 5.4 に示すようにポリシー設定支援ツールは耐侵入型アクセス制御システムの一部をなし，本システムは他に，ポリシーファイルとアクセス制御部からなる．アクセス制御部はポリシーファイルで決められたとおりにファイルアクセスを許可あるいは禁止するものであり，ポリシー設定支援ツールは利用者がポリシーファイルを管理できるようにする役割をもつ．

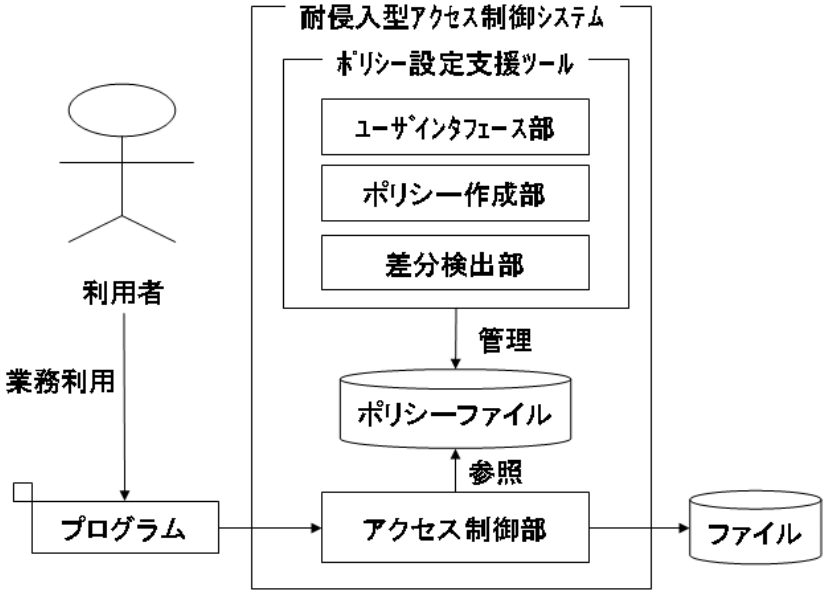

図 5.4: 耐侵入型アクセス制御システムの機能構成

ポリシー設定支援ツールの構成要素と役割は次に示すとおりである．

- ポリシー作成部
  前記（解決策１）（解決策２）にもとづきポリシー原案を自動生成すること

や，利用者が編集を完了したポリシーをポリシーファイルに保存する役割をもつ．

- 差分検出部
  前記（解決策３）にもとづく対話式のポリシー修正で，利用者にポリシーの修正案を提示するとともに，修正案に沿ってポリシーファイルのパラメータ変更を行う役割を持つ．

- ユーザインタフェース部
  前記ポリシー作成部が自動生成したポリシー原案の利用者への提示や，利用者による原案の編集を行うためのインタフェースを提供する．また，前記差分検出部が提供する対話式のポリシー修正インタフェースを利用者に提示する．

なおクライアントの利用形態には，１人１台が割り当てられる専用端末と，複数人で１台を利用する共用端末が考えられる．専用端末に本アクセス制御システムを導入する場合には，端末の利用者がそのまま本ツールの利用者となる．また共用端末に導入する場合には，管理者の役割を担う者がいると考えられることから，その管理者だけが本ツールの利用者となることとする．端末管理者が設定したポリシーにしたがって全ての端末利用者はクライアントを利用するものとなり，端末管理者以外はポリシーを一切変更することはできない．

5.5.3　ポリシー準自動設定機能

ポリシー準自動設定機能は図 5.5 に示す流れで処理を行い，ポリシーの初期設定を実現する．処理の流れを下記 (1)-(3) に示す．

(1) ポリシー原案の自動生成

利用者がポリシー設定支援ツールを起動すると，前記ポリシー作成部が前記（解決策１）に述べたパターンを許可するように（解決策２）のもとポリシー原案を自動生成する．

ところで 5.3.1 項に述べたポリシー設定によると，上記（解決策２）だけでは自動生成できない設定項目として，保護対象オブジェクトの絶対パス，ユーザ，アクセスタイプ，特徴値も決めなければならない．これらの設定項目については次のように考え，設定を簡易化するようにした．

(a) ユーザデータファイルは，利用者が決めたフォルダ以下にまとめて置かれることが多い．例えば Windows OS であれば「マイドキュメント」「デスクトップ」あるいは利用者が自ら定めたデータ用フォルダが考えられる．「マイド

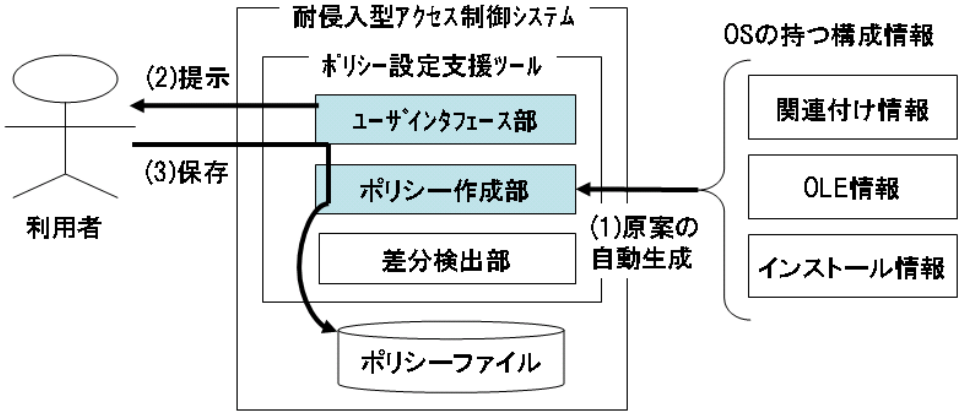

図 5.5: ポリシー準自動設定機能の処理の流れ

キュメント」「デスクトップ」を最初からポリシーに登録し，その他のフォルダの追加も容易にする．

(b) ユーザとアクセスタイプは，ポリシー設定簡略化のためクライアント向けには指定しない．ユーザとアクセスタイプの設定は，汎用 OS のファイルシステムの有する任意アクセス制御に委ねる．実際には両者のアクセス権チェックが行われるため，両者を組み合わせることで表 5.3 に示すようにサーバ向けと同等のきめ細かなアクセス制御を実現できる．

表 5.3: アクセス制御ポリシーの設定項目

設定項目	サーバ向け		クライアント向け
	耐侵入型 アクセス制御	耐侵入型 アクセス制御	任意アクセス 制御
オブジェクト	○	○	○
ユーザ	○	×	○
プログラム	○	○	×
特徴値	○	○	×
アクセスタイプ	○	×	○

○：設定する，×：設定しない

(c) プログラムの特徴値の検査を行うかどうかを，安全側を見て全てのプログラ

ムを対象に行うようにする．検査を不要とする場合には，簡略化のため一律に外せるようにする．

(2) ポリシー原案の編集

前記ポリシー作成部が生成したポリシー原案を利用者が確認し編集できるよう，前記ユーザインタフェース部が図 5.6 に示す画面を提供する．利用者は自動生成されたポリシー原案を編集すれば初期設定が完了する．以下に，原案の詳細と，利用者による編集項目を示す．なお前述した (1)(b) にもとづき，ユーザおよびアクセスタイプの設定項目はない．

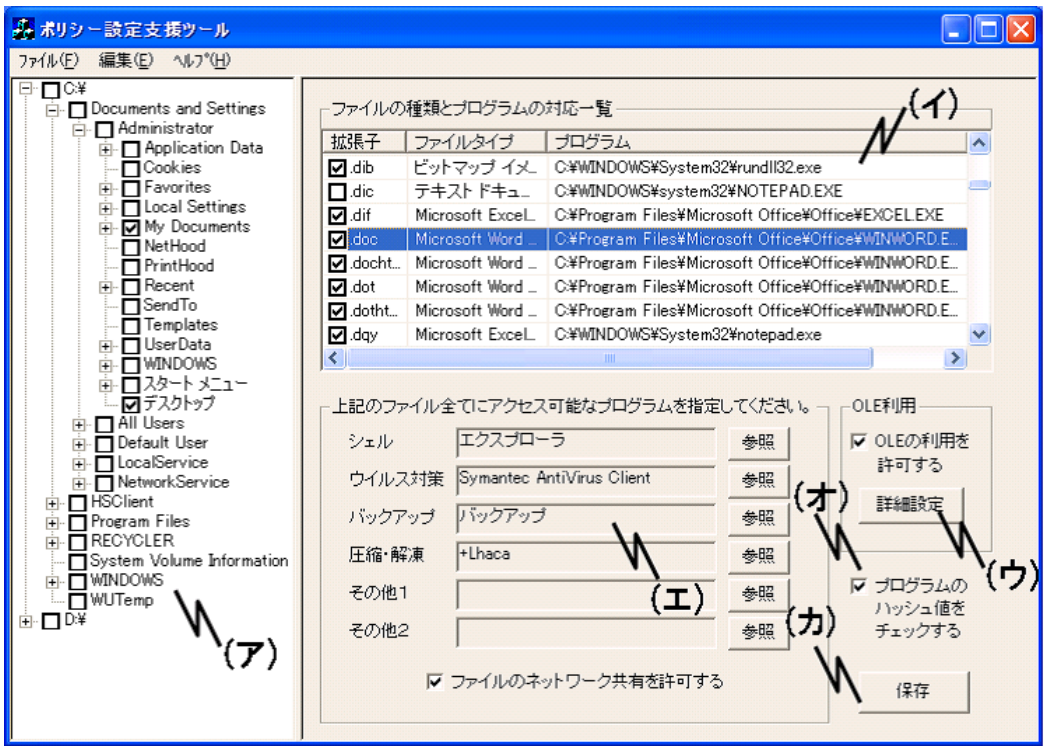

図 5.6: ポリシー編集画面

(ア) 監視対象とするフォルダの指定（図 5.6 の (ア)）

原案：前述した (1)(a) のもと,「マイドキュメント」「デスクトップ」を登録

編集：監視対象とするフォルダを辿ってチェックをつける

(イ) 保護対象とするファイルの指定（図 5.6 の (イ)）

原案：(解決策 2a) のもと，関連付け AP からのアクセスを全て許可

編集：保護対象としない拡張子のチェックを外す

(ウ)OLE 利用の許可と詳細設定（図 5.6 の (ウ)）

原案：(解決策 2a) のもと， OLE 対応の AP からのアクセスを全て許可

編集：「詳細設定」ボタンを押下して図 5.7 に示す OLE 利用許可の詳細選択ダイアログを開き，OLE 対応の AP の一覧の中からアクセスを許可しない AP のチェックを外す

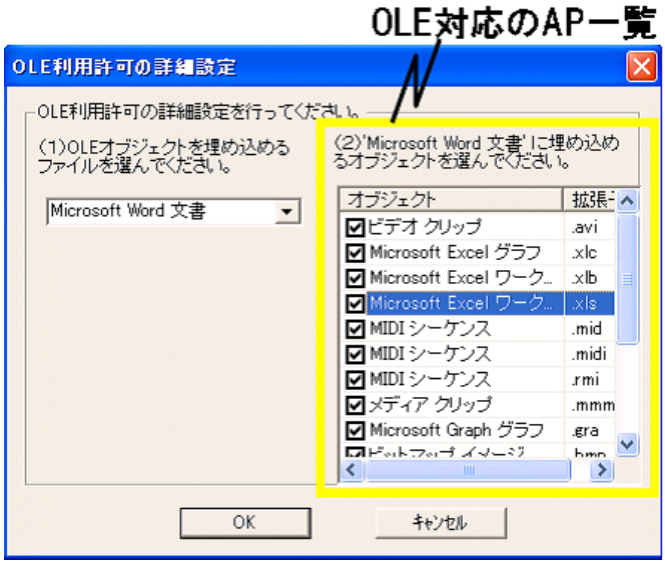

図 5.7: OLE 利用許可の詳細選択画面

(エ) 用途別プログラムの指定（図 5.6 の (エ)）

原案：(解決策 2b) のもと，OS 標準の用途別プログラムを登録

編集：「参照」ボタンを押下して図 5.8 に示す用途別プログラムの選択ダイアログを開き，(解決策 2c) に述べたようにインストールされたプログラムの一覧の中から該当するものを名称で選択する

(オ) プログラムの特徴値の検査実施の指定（図 5.6 の (オ)）

原案：前述した (1)(c) のもと，プログラムに対し一律に特徴値の検査を行う

編集：特徴値の検査を行わない場合にチェックを外す

(3) ポリシーファイルへの保存

利用者が図 5.6 の (カ) に示す「保存」ボタンを押下すると，前記ポリシー作成部がポリシーを前記ポリシーファイルに保存する．図 5.9 にポリシーの一部抜粋を示す．ポリシーファイルへの保存が完了すると，保存したポリシーにもとづいて前記アクセス制御部がファイルアクセスを許可あるいは禁止する．

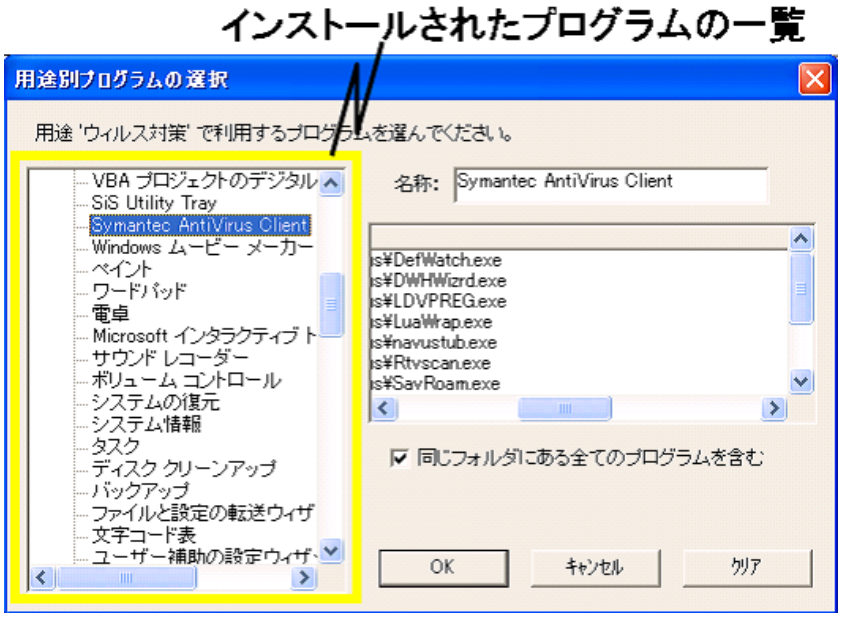

図 5.8: 用途別プログラムの選択画面

オブジェクト(フォルダ)
C:¥Admin¥ﾏｲﾄﾞｷｭﾒﾝﾄ¥
C:¥Admin¥ﾃﾞｽｸﾄｯﾌﾟ¥
D:¥Doc¥

ｵﾌﾞｼﾞｪｸﾄ (拡張子)	プログラム	特徴値	許可理由
*.doc	C:¥Prog¥Office¥Winword.exe	0x1234	関連付けAP
*.xls	C:¥Prog¥Office¥Excel.exe	0x2345	関連付けAP
*.xls	C:¥Prog¥Office¥Winword.exe	0x1234	OLE対応AP
.	C:¥Prog¥AntiVirus¥Scan.exe	0x3456	用途別-ｳｨﾙｽ対策

図 5.9: クライアント向けのファイルアクセス制御ポリシーの例

5.5.4 ポリシー対話型修正機能

ポリシー対話型修正機能は図 5.10 に示す流れで処理を行い，対話的なポリシーの修正を実現する．処理の流れを下記 (1)-(3) に示す．

(1) ポリシー違反の通知

前記アクセス制御部はポリシーと異なるファイルアクセスを検出したときに当ファイルアクセスを禁止し，さらに前記差分検出部へと通知する．差分検出部は，図 5.11 の (a) に示す不正アクセス監視画面を提示し，ポリシーに違反したアクセスが起きたことを利用者に通知する．

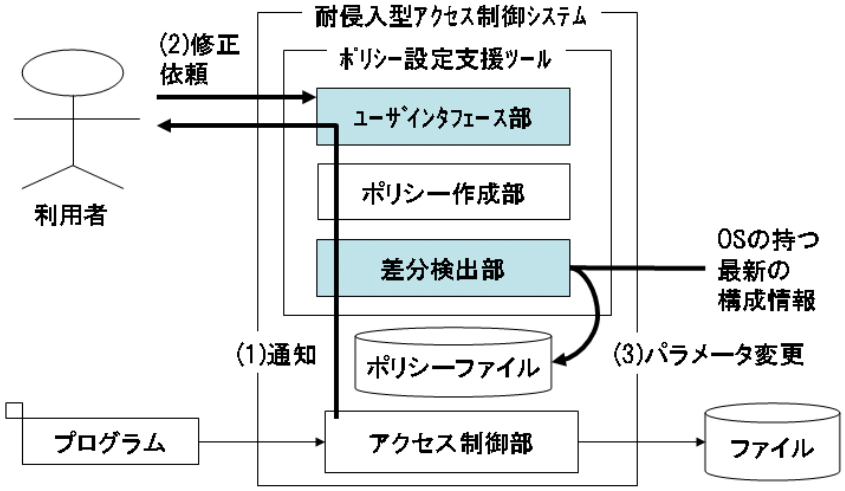

図 5.10: ポリシー対話型修正機能の処理の流れ

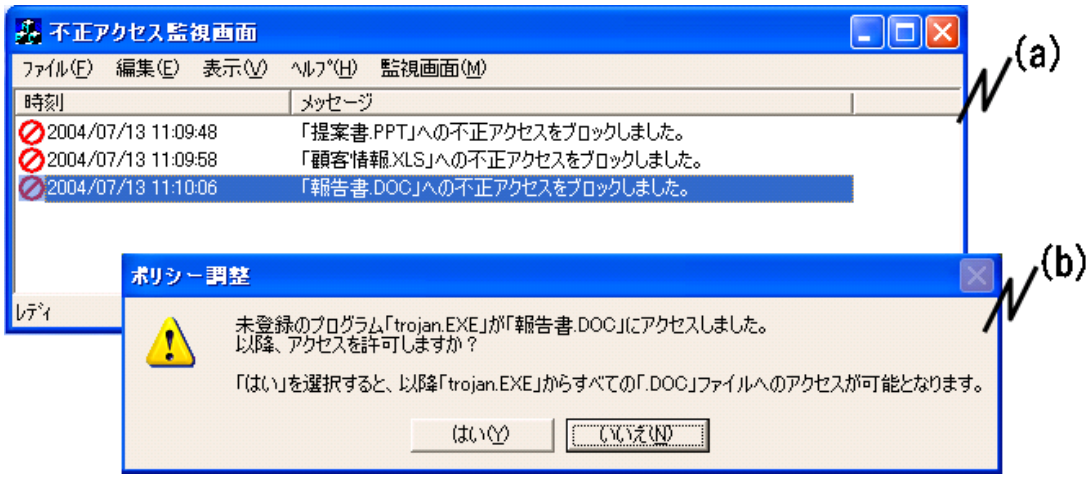

図 5.11: 対話的なポリシー修正画面

(2) 利用者からの修正依頼の受け付け

利用者は図 5.11 の (a) に示す不正アクセス監視画面に表示される情報をもとに，ポリシーを修正する必要性を判断する．ファイルアクセスが禁止されたままで良い項目については，利用者はそれ以上何もしない．必要なのに禁止されてしまっているファイルアクセスについては，利用者が図 5.11 の (a) に示す不正アクセス監視画面上で該当項目をクリック選択することで，前記ユーザインタフェース部が図 5.11 の (b) に示すポリシー調整ダイアログを表示し，そこで利用者は「はい」

ボタンを押下してポリシーの修正を依頼する．このような修正依頼の種類には，次に示すものがある．

(i) プログラム変更に伴う修正
既存アプリケーションのアップデートを行った場合，プログラムの特徴値がアップデート前と異なる場合がある．プログラムの特徴値を現在のものに修正する．

(ii) 関連付け情報変更に伴う修正
新規アプリケーションを追加する時にはレジストリの関連付け情報が追加・変更される場合がある．現在の関連付け情報をもとに導出したポリシーに修正する．

(iii) 例外的なアクセス許可と変更
5.5.3 項で述べたポリシー準自動設定機能でアクセス許可されたプログラム以外にも，利用者が例外的にファイルアクセスを許可したい場合がある．このような例外的なアクセスを許可するようポリシーを修正する．

(3) ポリシーファイルに対するパラメータ変更
前記差分検出部は，利用者の修正依頼を受けてから OS の持つ最新の構成情報を参照してポリシーの一部を再生成し，図 5.9 に示したポリシーファイル中のパラメータを変更する．変更が完了すると，変更後のポリシーにもとづいて前記アクセス制御部がファイルアクセスを許可あるいは禁止する．

5.5.5 開発結果の考察

開発したポリシー設定支援ツールを，ポリシー設定の容易性とポリシー原案の有効性の点から考察する．

ポリシー設定の容易性

ポリシー設定に必要な知識はポリシー原案の編集に必要な 5.5.1 項に述べた前提知識だけあれば良く，クライアントを使いこなせるような利用者にとって妥当なものだと考える．またポリシー設定に必要な手間は，ツールがポリシーを準自動で設定するために，利用者はポリシー原案をベースにチェックボックスのつけ外しや，候補一覧からの選択といった操作だけでポリシー設定を完了でき，初期設定に大きな手間はかからないと考える．GOMS 法（Goals, Operations, Methods and Selection rules）を用いて定量的評価を行った文献 [141] によるとポリシー設定完

了までに 10 分以内の操作時間で済む見通しを得た．さらに対話式のポリシー修正ができるため，ポリシー設定後も利用者が確認をとりながらクリック 2 回で修正することができ，修正にも手間がかからないと考える．

また 5.5.3 項に述べたポリシー原案によると，レジストリから読み取った拡張子の全てを対象に，その拡張子をもつファイルに対してアクセス制限を行うポリシーとなっている．一般にユーザデータファイルの拡張子は，レジストリに登録される拡張子がほとんどだと考えられるため，ポリシー原案をそのまま使うだけでもユーザデータファイルに対する保護を漏れなく実施することができると考える．

ポリシー原案の有効性

本アクセス制御システムでユーザデータファイルを保護していても，ポリシーで許可されたプログラム（以下，許可プログラムと称す）を不正プログラムが悪用してユーザデータファイルにアクセスすることも考えられる．このような悪用には（1）不正プログラムが許可プログラムの特徴値を変えずに感染する,（2）リモートから操作可能な許可プログラムを不正プログラムが操作する，といった状況がある．このような場合，提案方式では不正プログラムを原因としたアクセスと検知できない．このうち前記（1）は許可プログラムのソフトの脆弱性に起因するものと考えられ，そのため許可プログラムとして脆弱性の少ないプログラムを選定することが重要となる．また前記（2）についても，例えば P2P（Peer-to-Peer）ソフトのようにリモートから操作可能なプログラムを選定しないことが重要となる．

また本ポリシー設定支援ツールで設定したポリシーであったとしても，バッチ処理で使われるスクリプトや，文書ファイルに含まれるマクロに悪意のあるコードが入っている場合には，それらのコードによる悪意のある振る舞いを制御することはできない．なぜなら，耐侵入型アクセス制御はファイルシステムドライバの層でプログラムの振る舞いを制御するために，スクリプトやマクロといった上位アプリケーション層での振る舞いまでは制御できないからである．こうした上位アプリケーション層での振る舞いまで制御するためには，例えば Windows であればエクスプローラでの API フッキングを活用し，所定のスクリプトやマクロであれば実行を許可し，それ以外であれば実行を禁止するといった制御を行う方式が考えられる．

5.6 おわりに

本章では，クライアント上のユーザデータファイルを不正プログラムから保護することを目的とし，これまで筆者らがサーバ向けに開発してきた耐侵入型アク

セス制御をクライアントに応用したクライアント向けファイルアクセス制御方式を提案した．本方式は，多用途なクライアントに対して，正常アクセスの分析から多様なアクセスが代表的なパターンに分類できることを特定し，このパターンに基づくホワイトリスト型ポリシーの決定および設定を，OS の持つ構成情報を参照して準自動で行うものである．また本方式に基づくクライアント向けのポリシー設定支援ツールを試作した結果，ユーザデータファイルを漏れなく保護できるポリシーを，容易に設定できることを確認した．

また 5.4.2 項で述べた OS の持つ構成情報を参照したポリシー準自動設定の考え方は Windows OS だけに限らず，下記に示す情報を持つ OS に対してもそれらの情報を参照することでポリシーを準自動設定できるものとなる．

- ファイルへのアクセス手段として利用される可能性のあるプログラムの情報（例えば関連付け情報や OLE 情報）
- 用途別プログラムの情報（例えばインストール情報）

一例として Linux OS の場合には表 5.4 に示すように上記の各種情報を保有しており，これらの情報を参照すれば本論文で提案したポリシーを準自動設定できる見通しを得た．

表 5.4: ポリシー自動生成時に参照する OS 上の構成情報

ポリシー準自動生成時に参照する情報	Windows 2000/XP での参照箇所	Linux（Fedora Core 3）での参照箇所
関連付け情報	レジストリ	GNOME デトップのもつ MIME 設定ファイル
OLE 情報	レジストリ	OpenOffice アプリケーションのもつ OLE 設定ファイル
インストール情報	[スタート]-[プログラム] にあるショートカット一覧	「rpm -qa」コマンドの実行結果

第6章　結論

6.1　研究成果のまとめ

近年の脳科学の研究によると，ジョナ・レーラが提唱する「思考による窒息」とは次のように説明されている [142].

> どういう分野の活動でも，最高のレベルになると，無意識の果たす役割が大きくなる．何をするにしても初心者のうちは，脳のあちこちの部位が不規則にはたらいてしまう．ところが熟達してきて，無意識にできるようになると，はたらく部位が狭い範囲に限定され，さほど活発なはたらきは見られなくなる．つまり，熟練者は，少ない思考で大きな成果をあげるということだ．世界でもトップクラスという人なら，ほとんど「自動的に」動いている状態になっているはずだ．実際，スポーツ中継などでアナウンサーが選手の動きを「無意識の動き」と表現することはよくある．歌手にしろ，ゴルフ選手にしろ，**自分の動きを意識して考えてしまうとかえってうまくできなくなる**.

企業や組織におけるセキュリティ対策も，以前は業務の中に自然に無意識に組み込まれてきたものが，近年はセキュリティ脅威の質や量の変化に伴い，セキュリティを意識しなくてはならなくなっている．しかし，セキュリティを意識しすぎるあまり，本来業務がかえってうまくできなくなるという矛盾をはらんでいる．こうしたセキュリティを意識しすぎるために本来業務がうまくできない状態を「セキュリティによる窒息」と呼ぶことにする．

本研究で開発したオフィスセキュリティ技術をまとめるとともに，セキュリティによる窒息をどのように解決するかを議論する．

(1) 紙文書の漏えいリスクへの事前対応：重要印刷検出技術

オフィスのセキュリティ対策では，文書の漏えい防止のため，印刷出力コントロールが重要である．本研究では，文書内容を解析したうえで各種コントロールを行う DLP (Data Loss Prevention) 機構に着目し，印刷内容の解析を高速化した印刷コントロール機能の基本設計と開発結果を述べた．印刷文書を識別するために，文書 OCR と仮想プリンタドライバを組み合わせた画像処理方式（従来方式）では，フルテキストを取得するのに，仮想プリンタ

ドライバで行ったレイアウト配置を再び文書 OCR で解析し直すという処理の重複がある．そこで文書 OCR を使わずに，仮想プリンタドライバ内でレイアウト配置は無視しつつ，ページ内で処理される文字出力を処理順番の通りにつなげてフルテキストを取得する文字コード処理方式（提案方式）を考案した．提案方式を Windows XP 上で実装することで，仮想プリンタドライバでレイアウト配置を無視してもフルテキスト取得への影響が小さいことを確認し，印刷速度の低下が 0.4 秒程度以下に抑えられる見通しを得た．

(2) 紙文書の漏えいリスクへの事後対応：印刷監視・調査技術

もしオフィスからの情報漏えいが発覚すると，調査員はどの文書が漏えいしたか，誰が漏えいしたかを調べる必要がある．印刷による漏えいが疑われる場合，従来のフォレンジックプロセスでは作業工数を要する一方で，PC などに残されたデータからいつ，誰が，何を印刷したかを調査することが困難であった．本研究では，調査を効率化するために日常的な監視を加えた拡張フォレンジックプロセスを提案し，前記プロセス実現に向けた印刷監視システムの開発結果を述べた．印刷監視システムでは，漏えいした紙文書との一致性確認と共に，大量の印刷ログからの絞り込みを行うため，ページ単位の画像とフルテキストの両データを記録し，全文検索を行った．印刷監視システムの利用により，1 週間以内に一次報告を行う漏えい調査シナリオを想定した場合に，従来のフォレンジックプロセスで約 4 名を要していた作業工数が，1 名で実施可能な見通しを得た．

(3) 未知ウイルス感染リスクへの事前対応：ウイルス封じ込め技術

コンピュータのネットワーク化が進み社会基盤を担う一方で，ウイルス・ワーム感染は深刻な問題である．とくにウイルス・ワームがコンピュータ上の情報資産を外部に漏えい及び改ざんした場合の被害は甚大である．このためウイルス対策ソフトの導入やセキュリティパッチ適用が一般に行われているが，ワクチンやパッチが間に合わない時間には情報資産が無防備になるという問題がある．この問題に対処するため筆者らはこれまでサーバ向けに，仮にコンピュータが侵入された場合にも情報資産を保護する耐侵入型アクセス制御を開発してきた．本アクセス制御は，情報資産にアクセスするプログラムを制限することで，情報資産の改ざんと漏えいを防止する．しかし情報資産はネットワークにおいてサーバに限らずクライアントにも多数存在する．そこで本研究では，耐侵入型アクセス制御をクライアントに適用したクライアント向けファイルアクセス制御方式を提案した．クライアントに適用する上で，多用途なクライアントではポリシーの決定に必要な正常アクセスの把握が困難となり，一般利用者でもポリシーを設定できるように専門的な知識

や煩雑な手間を不要とすることが課題となる．これに対し，正常アクセスの分析から多様なアクセスが代表的なパターンに分類できることを特定し，このパターンに基づくポリシー決定および設定を，OS の持つ構成情報を参照して準自動で行う方式とした．

以上述べてきたオフィスセキュリティ技術を使うと，従業員に対して重要印刷の気づきを与えることや，端末（PC）での印刷を監視すること，PC での未知ウイルスに対する封じ込めというオフィスでのよくあるリスクに対して，上長・マネージャは上記技術を実装したツールを従業員が使っているかどうかを観察するだけで済む．よって，これらのリスクに対するセキュリティ対策をツール任せにできる．近年の端末監視ツール [108] を活用すれば，各 PC へのインストール有無の確認やツールが常時起動していることの確認は十分に実装できる．一方，従業員もツールに従っていれば，通常業務には大きな負担をかけずに，業務に組み込まれた自然な形でセキュリティ対策を実施できる．このように上長・マネージャと従業員の両方にとって，オフィスセキュリティ技術は「セキュリティによる窒息」の解消に資する技術である．

6.2 議論

本研究の成果であるオフィスセキュリティ技術は，1 章の研究の範囲で述べた「Weakest Link」「セキュリティTCO」「リスク定量化」の観点からすると，ヒューマンファクタによる情報漏えいリスクやウイルス感染リスクに有効である．その一方で，オフィスセキュリティの範囲は広いため，近年の状況や今後の変化からすると，さらに解決すべき課題もいくつかある．ここでは，オフィスセキュリティに関する今後の研究の方向性を議論する．

6.2.1 オフィスセキュリティと Weakest Link

2000 年代以降，セキュリティ対策の Weakest Link だと言われてきたワークステーション（端末側）やヒューマンファクタの問題は，今後も引き続き問題であり続け，加えて問題の質をますます複雑にすると考えられる．以下に示す 3 点から議論する．

- 組織面の変化
- ミッションやビジネスプロセスの変化
- 情報システムの変化

組織面の変化

オフィスは企業や組織に属するものである．そうした企業や組織に関して，特に民間企業では企業の買収・合併が繰り返し行われてきた．また自治体においても「平成の大合併」により多くの市町村が合併あるいは分割された．オフィスが属する企業や組織が変化することで，オフィスも拡大，縮小，移動を伴うことが考えられる．一度確立したオフィスセキュリティも，こうした拡大，縮小，移動に伴い追随する必要がある．

企業や組織レベルの拡大，縮小，移動に伴い，オフィスで働く従業員の人材流動も活発化する．異動する人材は，異動するたびに異なるセキュリティポリシーの下で働かなければならない．そのためセキュリティポリシーの解釈の違いや明文化されていない企業風土への対応など，オフィスセキュリティの変化を従業員側で吸収しなければならない余地が大きくなる．

ミッションやビジネスプロセスの変化

近年，日本企業のビジネスプロセスもいくつかの点で変化が起きている．

- グローバル化により，オフィスを海外に設けることの増加
- 外部委託により，外部委託先にまで自組織と同等のセキュリティを求めることの増加
- オープンイノベーション（自社技術だけでなく他社が持つ技術やアイデアを組み合わせて，革新的な商品やビジネスモデルを生み出すこと）のために，他社との技術交流の増加

このため，遠隔地のオフィスのセキュリティ確保や，オフィスの境界のあいまい化への対応が必須である．

また近年，勤務形態も変化しつつあり，節電対策や計画停電対応のために，在宅勤務も広く認められるようになった [143]．在宅勤務時には仕事とプライベートとの境界を持ちにくくなる．さらに下記に示すような，仕事とプライベートとの境界をきめ細かく切り替える「ライフスライス」という考えも発表されている [144]．働く場所や働く時間帯に応じてセキュリティ対策を自在に切り替えるようなセキュリティ対策も今後重要となる．

例えばワークスタイルにしても 10 年前は仕事とプライベートがきっちり分かれていて，オフィスにいる間は仕事，家に帰ればプライベートだった．しかし，いまは**仕事とオフィスが細かくスライスされて相互に混じり合っている**．わ

たしはこの状態を“ ライフスライス ”と呼んでいる（Citrix 社長兼 CEO Mark Templeton 氏）.

さらに近年，営業秘密の管理強化の観点から，産業スパイなどのリスクに対して法的保護を受けるための前提条件として，下記に示すような秘密管理性まで求められつつある [145].

営業秘密を適切に管理することは、不正競争防止法による営業秘密保護のための要件である秘密管理性の重要な要素となるため、営業秘密としての法的保護を受けるための前提条件である。また、**いかに重要な情報であったとしても、その情報が秘密として適切に管理されていなければ、営業秘密としての法的保護を受けることはできない。**

そこで、事業者においては、秘密情報が漏えいした場合に、事後的に法的保護を受けることができる実効的な管理をすることが望ましい。

上記の秘密管理性の要件を満たすためには，さらに (1) 情報にアクセスできる者を制限すること，(2) 情報にアクセスした者にそれが秘密であると認識できること，を満たす必要がある．そのため，営業秘密に該当するような情報は作成した時点で，何らかの「秘密であると認識できる」ような印を付与される必要がある．情報の持ち出し段階だけでなく，こうした作成段階まで含めたセキュリティ対策も今後重要となる．

情報システムの変化

これまでの情報システムはクライアント・サーバという分散型で進歩してきた一方で，近年のクラウドコンピューティング化とスマートフォンの普及は，集中型へと変化しつつあると言える．分散型システムでは，サーバは 24 時間 365 日稼動する一方で，クライアント側は就業時間外は電源を切ることが多かった．一方，スマートフォンは PC に比べて常時電源が入っており，また常時ネットワークに接続している．さらに BYOD（Bring Your Own Device）と呼ばれるように，従業員が私物の端末を企業内に持ち込んで業務に活用する機会も増加することが見込まれる [146]．こうしたスマートフォンの特性から，情報漏えいやウイルス感染のリスクは高まると言える．スマートフォン向けのセキュリティは本論文の執筆時点では発展途上であり，今後のセキュリティ技術開発が期待される．

6.2.2 オフィスセキュリティとセキュリティTCO

1 章に述べたセキュリティTCO は，図 6.1 に示すように，構成員と時間軸で広がりを示した．今後，セキュリティTCO はヒューマンファクタの影響によります

ます大きくなることが予想される．理由は，以下に述べる空間的な広がりと時間的な広がりのためである．

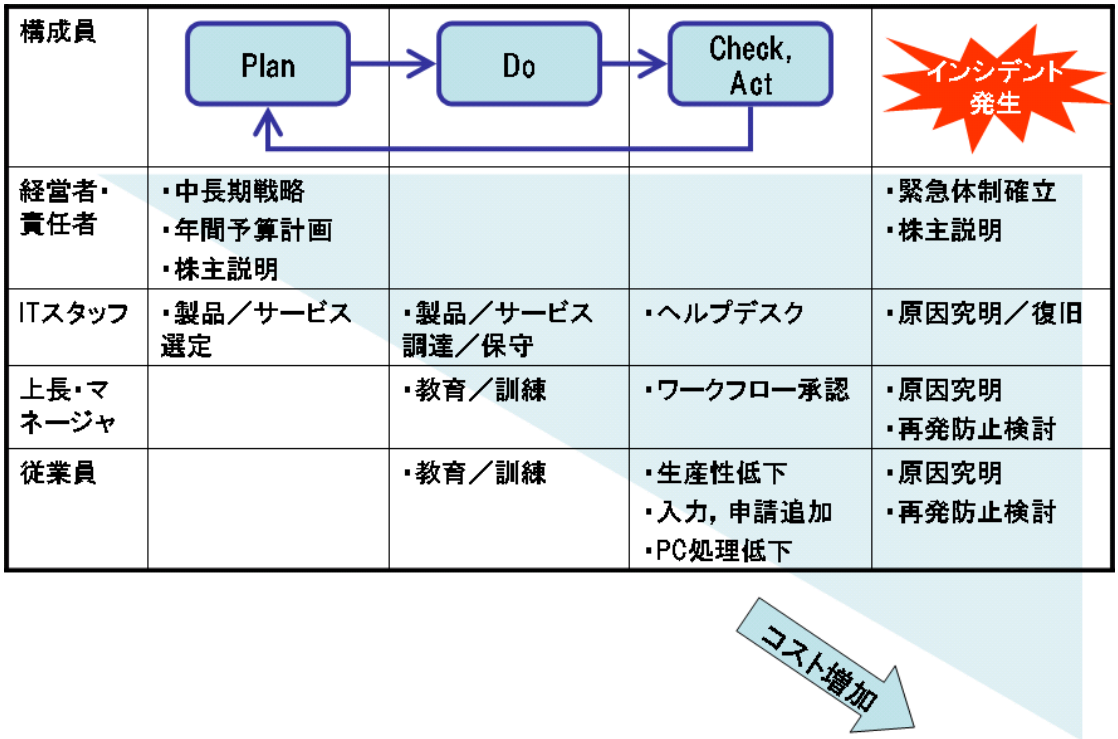

図 6.1: 企業や組織におけるセキュリティTCO（図 1.4 を再掲）

空間的な広がり

Weakest Link の議論でも述べたように，今後の企業や組織はグローバル化やオープンイノベーション化が避けられない．遠隔地のオフィスやオフィス境界のあいまい化によって，セキュリティTCO はますます大きくなる．

時間的な広がり

2011 年 3 月 11 日に起きた東日本大震災では，震災直後には避難命令によってオフィスへの立ち入りが一切禁止されたこともあった．また，震災直後の停電や，その後の電力不足による計画停電によって，電源が提供されないこともあった．このような，発生頻度は限りなく低いが影響が限りなく大きいような大災害時まで考慮したオフィスセキュリティは，これまでのところほとんど議論されることが

なかったと考えられる．例えば，震災直後での安否確認プロセスひとつをとってみても，オフィスに在室が確認されていれば安否確認メールの送信をしないことで，メールサーバやネットワークの負荷を下げる，といったことまで考慮が必要と考えられる．

また同じく東日本大震災直後では，デマ情報も流れ，多くの人を混乱と不安に陥れた [147]．デマ情報を収束させるには，正式な情報筋からの情報発信を待つといった手間のかかるプロセスを経る必要がある．技術での解決には限界があると考えられる分野であり，そのためヒューマンファクタへの影響はますます大きくなる．

6.2.3 オフィスセキュリティとリスク定量化

企業や組織を取り巻く経済環境は，近年，非常に大きく変化している．

- 2008 年，リーマンショックを契機とする金融危機とその後の世界同時不況
- 2011 年，東日本大震災による，地震，津波，原子力発電所事故からの復旧・復興
- 2012 年，欧州債務危機の深刻化，2009 年に発生したギリシャ危機にはじまり，イタリアやスペインの国家財政危機など

このような急激な経済環境の変化は，経営者だけでなく従業員にも多大なストレスを与える．ストレスにより従業員が悪意の動機を持つことも容易に想像される．もし明日解雇されるとしたら，IT 管理者の 88%が会社の機密情報を持ち出すと回答したことは既に述べた [28]．こうした悪意の動機を持つことにつながる要因は今後ますます増え，そのためリスクの定量化もさらに測ることが困難になると考えられる．

6.3 今後の課題

前節で述べた「Weakest Link」「セキュリティTCO」「リスク定量化」の議論からすると，今後のオフィスセキュリティ研究は，時間的および空間的に広がるオフィスセキュリティおよび変化するオフィスセキュリティに関し，技術を使って効率良くセキュリティを実現することが課題である．つまり以下に示す 2 点に大きく整理できる．

技術を使ってのオフィスセキュリティの向上

セキュリティポリシーをトップからボトムへと流す動脈系のセキュリティと，オフィスの現場でのリスクやインシデントをボトムからトップへと流す静脈系のセキュリティの確立．技術を活用して動脈系及び静脈系セキュリティを効率良く低い TCO で実現すること（図 6.2）．

オフィスで使われる新技術への対応

クラウドコンピューティング環境の利用やスマートフォンの普及に伴う業務利用といった新たな技術に，オフィスセキュリティとして対応すること．

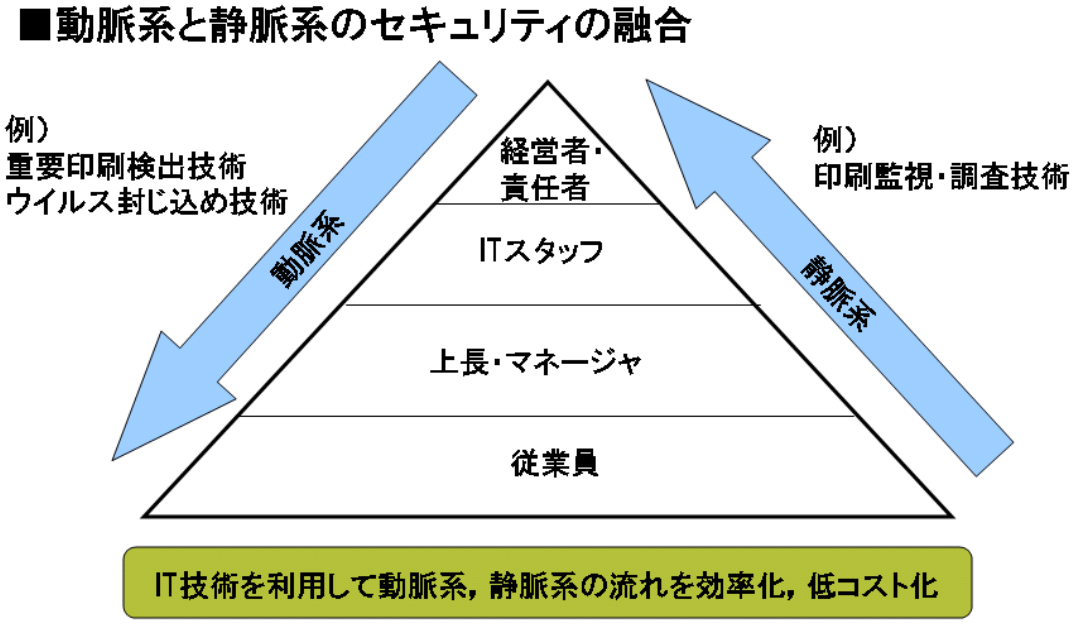

図 6.2: 今後のオフィスセキュリティ研究の方向性

これまでは IT 化が進歩するにつれてオフィスでの業務も IT 化が進み，IT 化すれば業務も効率化できると信じられてきたと考えられる．しかし実際には，IT 化された業務において新たなセキュリティリスクが発生し，オフィスセキュリティを後追いで考えざるを得なかった．今後は，本来の業務に対して IT がどう役立つかを吟味した上で，真に業務に役立つ IT だけを取り入れるなど，流行の IT 化に振り回されないオフィスセキュリティの設計を進めるべきと考える．

参考文献

[1] 一般財団法人日本情報経済社会推進協会（JIPDEC）プライバシーマーク事務局. プライバシーマーク制度. http://privacymark.jp/. 2012年5月確認.

[2] 一般財団法人日本情報経済社会推進協会（JIPDEC）情報マネジメントシステム推進センター. 情報セキュリティマネジメントシステム適合性評価制度. http://www.isms.jipdec.or.jp/. 2012年5月確認.

[3] 日本事務機.　情報セキュリティソリューション Seplus.　http://www.securityplus.jp/. 2012年5月確認.

[4] 高橋郁夫. Use of Digital Forensics and the legal problems in information leakage incident response in japan. *Proceedings of 4th Annual IFIP WG 11.9 International Conference on Digital Forensics - Short Papers* -, pp. 65–72, Jan. 2008.

[5] ファイリングの部屋. 13-2-2. 政府のペーパーレス化実施状況. http://www.amy.hi-ho.ne.jp/kido/paperless.htm. 2012年5月確認.

[6] NPO日本ネットワークセキュリティ協会. 2010年情報セキュリティインシデントに関する調査報告書〜個人情報漏えい編〜. http://www.jnsa.org/result/incident/2010.html. 2012年5月確認.

[7] トレンドマイクロ. 物理アプライアンスの限界　目で見る仮想アプライアンスの魅力. http://jp.trendmicro.com/jp/solutions/enterprise/va/migration/. 2012年5月確認.

[8] I. Arce. The weakest link revisited [information security]. *Security & Privacy, IEEE*, Vol. 1, No. 2, pp. 72–76, 2003.

[9] 経済産業省. 情報システム・ソフトウェアの信頼性及びセキュリティの取組強化に向けて　〜豊かで安全・安心な高度情報化社会に向けて〜　ー中間報告書ー　エグゼクティブサマリ. http://www.meti.go.jp/press/20090528001/20090528001-4.pdf. 2012年5月確認.

[10] 月刊 総務 2011 年 06 月号 [雑誌]. ナナ・コーポレート・コミュニケーション, May 2011.

[11] W. Sonnenreich, J. Albanese, and B. Stout. Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and Practice in Information Technology*, Vol. 38, No. 1, pp. 45–56, 2006.

[12] 警察庁. 不正アクセス行為対策等の実態調査. http://www.npa.go.jp/cyber/research/. 2012 年 5 月確認.

[13] Deborah Russell and G.T.Gangemi Sr. コンピュータセキュリティの基礎 (Nutshell handbooks). アスキー, Nov. 1994.

[14] 経済産業省. コンピュータウイルス対策基準. http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm. 2012 年 5 月確認.

[15] J.J. Gonzalez and A. Sawicka. A framework for human factors in information security. In *WSEAS International Conference on Information Security, Rio de Janeiro*, 2002.

[16] M. Egan. Information security and the human factor. *ISACA Journal*, Vol. 3, pp. 1–2, 2005.

[17] D. Trcek. Security models: Refocusing on the human factor. *Computer*, Vol. 39, No. 11, pp. 103–104, 2006.

[18] 川越秀人, 内田勝也. 情報セキュリティのヒューマンファクタ. 情報処理学会研究報告. CSEC,[コンピュータセキュリティ], Vol. 2008, No. 45, pp. 7–12, 2008.

[19] ITPro. 「セキュリティ予算は，全 IT 予算の 3〜7 %が妥当」，米 Gartner のセキュリティ担当リサーチャー. http://itpro.nikkeibp.co.jp/article/Interview/20071203/288555/. 2012 年 5 月確認.

[20] NTT データ先端技術株式会社. 米国における情報セキュリティの動き＜第 1 回＞. http://security.intellilink.co.jp/article/security/080515.html. 2012 年 5 月確認.

[21] KDDI 総研. 情報セキュリティ投資に対する企業の意志決定. http://www.kddi-ri.jp/pdf/KDDI-RA-200611-22-PRT.pdf. 2012 年 5 月確認.

[22] デジタル・フォレンジック・コミュニティ2008国内事例報告. 内部統制評価に有効な証跡管理（エンタープライズ・フォレンジック）の研究開発　研究成果の紹介. http://www.digitalforensic.jp/archives/2008/811.pdf. 2012年5月確認.

[23] 一般財団法人日本情報経済社会推進協会情報マネジメント推進センター. JIS Q 27001:2006　情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項. 一般財団法人　日本規格協会, 2006.

[24] 財団法人日本情報処理開発協会. ISMSユーザーズガイド - JIS Q 27001:2006 (ISO/IEC 27001:2005) 対応 - リスクマネジメント編. http://www.isms.jipdec.or.jp/doc/JIP-ISMS113-21.pdf. 2012年5月確認.

[25] 岡本卓馬. 情報セキュリティにおけるリスクの定量化手法, pp. 86–96. Unisys Technology Review 第86号, Aug. 2005.

[26] @IT. セキュリティ製品の基礎知識と導入手引き【連載】情報セキュリティ運用の基礎知識　第4回 経営層にセキュリティの重要性を納得させる. http://www.atmarkit.co.jp/fsecurity/rensai/info04/info01.html. 2012年5月確認.

[27] 法務省.　平成23年版 犯罪白書 －少年・若年犯罪者の実態と再犯防止－. http://hakusyo1.moj.go.jp/jp/58/nfm/mokuji.html. 2012年5月確認.

[28] ITpro. 大半のIT管理者は「明日解雇されるなら機密情報を持ち出す」–米調査. http://itpro.nikkeibp.co.jp/article/NEWS/20080828/313609/. 2012年6月確認.

[29] Bruce Schneier, ブルース・シュナイアー. 暗号の秘密とウソ. 翔泳社, Oct. 2001.

[30] ブルース・シュナイアー. セキュリティはなぜやぶられたのか. 日経BP社, Feb. 2007.

[31] Adams, A. and Sasse, M.A. Users are not the enemy. *Communications of the ACM*, Vol. 42, No. 12, pp. 40–46, 1999.

[32] 加藤岳久, 中澤優美子, 漁田武雄, 山田文康, 山本匠, 西垣正勝. 本人認証技術におけるユーザの性格とセキュリティ意識との相関に関する考察. 情報処理学会論文誌, Vol. 52, No. 9, pp. 2537–2548, 2011.

[33] 中澤優美子, 加藤岳久, 漁田武雄, 山田文康, 西垣正勝. Best Match Security: 個人に適したセキュリティ対策を講じるシステムの提案. 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, Vol. 108, No. 162, pp. 133–138, 2008.

[34] 中澤優美子, 加藤岳久, 漁田武雄, 山田文康, 山本匠, 西垣正勝. Best Match Security: 性向とパスワード認証のセキュリティ意識との相関に関する検討 (セッション 1-B: セキュリティ応用技術). 情報処理学会研究報告. マルチメディア通信と分散処理研究会報告, Vol. 2009, No. 20, pp. 43–48, 2009.

[35] 中澤優美子, 加藤岳久, 漁田武雄, 山田文康, 山本匠, 西垣正勝. Best Match Security: 性格と本人認証技術のセキュリティ意識との相関に関する検討. 情報処理学会研究報告. CSEC,[コンピュータセキュリティ], Vol. 2010, No. 21, pp. 1–8, 2010.

[36] 平野亮, 森井昌克. パスワード運用管理に関する考察および提案とその開発 (情報セキュリティ). 電子情報通信学会技術研究報告: 信学技報, Vol. 111, No. 285, pp. 129–134, 2011.

[37] Carstens, D.S. and McCauley-Bell, P.R. and Malone, L.C. and DeMara, R.F. Evaluation of the human impact of password authentication practices on information security. *Informing Science: International Journal of an Emerging Transdiscipline*, Vol. 7, pp. 67–85, 2004.

[38] Bowen, B.M. and Devarajan, R. and Stolfo, S. Measuring the human factor of cyber security. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, pp. 230–235. IEEE, 2011.

[39] Sun, X. and Liu, Y. and Wang, J. Impact of human factors on email worm propagation. In *Web Society, 2009. SWS'09. 1st IEEE Symposium on*, pp. 102–107. IEEE, 2009.

[40] Islam, S. and Dong, W. Human factors in software security risk management. In *Proceedings of the first international workshop on Leadership and management in software architecture*, pp. 13–16. ACM, 2008.

[41] Fujikawa, M. and Aoki, H. and Nishigaki, M. and Yoshizawa, M. and Tsujii, S. Design of Office Security System that is capable of Detecting Unauthorized Persons Wearing Office Uniforms. Proc. of the 2nd Int 'l Conf. on Safety and Security Systems in Europe, 2007.

[42] 石垣陽, 松永昌浩, 茅野貢. 恐喝・詐欺・故意・過失を防ぐ適応的認可手法. 情報処理学会コンピュータセキュリティシンポジウム 2010 論文集, pp. 495–500, 2010.

[43] 荒井正人, 田中英彦. 機密情報共有に有用な情報フロー制御モデルの提案. 情報処理学会論文誌, Vol. 51, No. 2, pp. 635–647, 2010.

[44] 小野良司, 桜井鐘治, 木村俊之, 撫中達司. 機密情報持出し制御システムの試作とその評価 (オフィスインフォメーションシステム及び一般). 電子情報通信学会技術研究報告. OIS, オフィスインフォメーションシステム, Vol. 105, No. 650, pp. 43–47, 2006.

[45] 齋藤良平, 山川裕大, 久保山哲二, 安田浩. PC 操作ログからの従業員 PC 利用パターンのクラスタリング (ログ活用・情報検索, グループウェアとネットワーク, ライフログ活用技術, 一般). 電子情報通信学会技術研究報告. LOIS, ライフインテリジェンスとオフィス情報システム, Vol. 111, No. 50, pp. 9–13, 2011.

[46] 小林透, 豊田真智子, 市川裕介. 端末操作ログを対象にした情報漏洩につながる危険行動高速抽出方式 (ライフログ, ライフログ活用技術, オフィスインフォメーションシステム, ライフインテリジェンス, 一般). 電子情報通信学会技術研究報告. LOIS, ライフインテリジェンスとオフィス情報システム: IEICE technical report, Vol. 110, No. 450, pp. 19–24, 2011.

[47] 榊原裕之, 桜井鐘治. ログ分析による情報漏洩監視. 情報処理学会研究報告. CSEC,[コンピュータセキュリティ], Vol. 2011, No. 23, pp. 1–6, 2011.

[48] 芝口誠仁, 稲場太郎, 中山佑輝. 仕事量及び利便性低下度に着目したセキュリティ対策選定手法 (ライフインテリジェンスとオフィス情報システム). 電子情報通信学会技術研究報告, Vol. 109, No. 39, pp. 61–66, 2009.

[49] 社団法人ニューオフィス推進協議会. オフィスセキュリティマーク認証基準 (Ver3.0). http://www.nopa.or.jp/security/pdf/osm_v3.pdf. 2012 年 5 月確認.

[50] 池田宏, コクヨ S&T セキュリティ推進室. セキュリティ時代の文書管理 - コクヨの「危機回避」ファイリング術. 日経 BP 企画, Apr. 2006.

[51] 石島正勝. 情報の権限付与と共有範囲を考える (< 特集 > ノウハウの蓄積と伝達). 情報の科学と技術, Vol. 56, No. 1, pp. 19–24, 2006.

[52] 三品拓也, 勝野恭治, 吉濱佐知子, 工藤道治. 来歴に基づくマルチレベルセキュリティ文書管理システム. 情報処理学会論文誌, Vol. 49, No. 9, pp. 3062–3073, 2008.

[53] 今井正樹, 上原哲太郎, 侯書会, 津田侑, 喜多一. 情報漏洩元の特定を可能とする電子文書管理システムの提案 (サービス管理, 運用管理技術, セキュリティ管理, 及び一般). 電子情報通信学会技術研究報告. ICM, 情報通信マネジメント, Vol. 111, No. 30, pp. 19–24, 2011.

[54] S. Brin, J. Davis, and H. Garcia-Molina. Copy detection mechanisms for digital documents. In *ACM SIGMOD Record*, Vol. 24, pp. 398–409. ACM, 1995.

[55] N. Shivakumar and H. Garcia-Molina. SCAM: A copy detection mechanism for digital documents. 1995.

[56] 芹田進, 藤井康広, 甲斐賢, 村上隆夫, 本多義則. ファイル伸縮に耐性のある類似ハッシュ算出方式の考察 (情報セキュリティ, ライフログ活用技術, ライフインテリジェンス, オフィス情報システム, 一般). 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, Vol. 110, No. 281, pp. 31–36, 2010.

[57] 道井將, 川出篤, 村中宏彰. セキュアなプリンティングシステムのオフィスへの導入のための改良と評価 (ライフインテリジェンスとオフィス情報システム). 電子情報通信学会技術研究報告, Vol. 109, No. 379, pp. 57–62, 2010.

[58] 川出篤, 村中宏彰, 道井將, 久保田直樹, 松山浩, 小澤光興, 横山朝征, 新村正明, 國宗永佳, 不破泰. オフィスにおけるセキュアなプリンティングシステムの認証機能とユーザおよび機器のデータ管理機能の既存システムへの統合 (オフィスシステム, ライフログ活用技術, オフィス情報システム, 情報通信マネジメント, 一般). 電子情報通信学会技術研究報告. LOIS, ライフインテリジェンスとオフィス情報システム: IEICE technical report, Vol. 109, No. 379, pp. 63–68, 2010.

[59] 村中宏彰, 川出篤, 道井將, 久保田直樹, 松山浩, 小澤光興, 横山朝征, 新村正明, 國宗永佳, 不破泰. オフィスにおける既存システムとの連携によるセキュアなプリンティングシステムのサーバレス化の提案と評価 (オフィスシステム, ライフログ活用技術, オフィス情報システム, 情報通信マネジメント, 一般). 電子情報通信学会技術研究報告. LOIS, ライフインテリジェンスとオフィス情報システム: IEICE technical report, Vol. 109, No. 379, pp. 69–74, 2010.

[60] 北井大樹, 名古大介, 川出篤, 道井將, 村中宏彰, 桑原大樹, 新村正明, 國宗永佳, 松山浩, 小澤光興ほか. 出先機関向け税証明発行システムにおけるセキュアなプリンティングシステムの導入と評価 (システムセキュリティ). 電子情報通信学会技術研究報告. OIS, オフィスインフォメーションシステム, Vol. 108, No. 397, pp. 33–38, 2009.

[61] 名古大介, 北井大樹, 川出篤, 道井將, 村中宏彰, 桑原大樹, 新村正明, 國宗永佳, 松山浩, 小澤光興ほか. セキュアなプリンティングシステムにおける出力プリンタ制限機能の拡張について (システムセキュリティ). 電子情報通信学会技術研究報告. OIS, オフィスインフォメーションシステム, Vol. 108, No. 397, pp. 39–44, 2009.

[62] 金井洋一, 斉藤敦久. ポリシーベース・ドキュメントセキュリティシステムの開発. リコーテクニカルレポート, No. 30, pp. 128–135, 2004.

[63] 的場和男. デジタル複合機におけるネットワークセキュリティへの対応. *Konica Minolta technology report*, Vol. 3, pp. 57–61, 2006.

[64] 鳥山秀之, 石黒和宏, 浅野基広. 地紋プリントを利用したペーパーセキュリティー機能. *Konica Minolta technology report*, Vol. 7, pp. 88–92, 2010.

[65] 福田康裕, 松本勉. 紙から固有な値を抽出する可視光人工物メトリック・システムの一方式 (情報セキュリティ, ライフログ活用技術, ライフインテリジェンス, オフィス情報システム, 一般). 電子情報通信学会技術研究報告. LOIS, ライフインテリジェンスとオフィス情報システム: IEICE technical report, Vol. 110, No. 282, pp. 37–43, 2010.

[66] ITmedia. オフィスの PC は勤務時間の約 3 割が未使用状態――ナナオが調査. `http://plusd.itmedia.co.jp/pcuser/articles/0911/30/news069.html`. 2012 年 5 月確認.

[67] 独立行政法人情報処理推進機構. 「IT コーディネータが見た中小企業等におけるクラウドサービス利用上の課題・導入実態」調査報告書. `http://www.ipa.go.jp/about/press/20120417.html`. 2012 年 5 月確認.

[68] 独立行政法人情報処理推進機構（IPA）. IPA テクニカルウォッチ『新しいタイプの攻撃』に関するレポート～Stuxnet（スタックスネット）をはじめとした新しいサイバー攻撃手法の出現～. `http://www.ipa.go.jp/about/technicalwatch/20101217.html`. 2012 年 5 月確認.

[69] 独立行政法人 情報処理推進機構 技術本部セキュリティセンター. IPA テクニカルウォッチ　組織の内部不正防止への取り組み. http://www.ipa.go.jp/about/technicalwatch/pdf/120315report.pdf. 2012 年 5 月確認.

[70] 桜井哲夫. 知の教科書　フーコー (講談社選書メチエ). 講談社, May 2001.

[71] ウィキペディア. パノプティコン. http://ja.wikipedia.org/wiki/%E3%83%91%E3%83%8E%E3%83%97%E3%83%86%E3%82%A3%E3%82%B3%E3%83%B3. 2012 年 5 月確認.

[72] キヤノン株式会社. 文字処理装置，文字処理方法及び記録媒体. 特開 2006-261907 号, 2006-09-28.

[73] McAfee. McAfee Application Control. http://www.mcafee.com/japan/products/application_control.asp. 2012 年 5 月確認.

[74] Lumension. ホワイトリスト方式エンドポイントセキュリティ. http://www.endpointsecurity.jp/. 2012 年 5 月確認.

[75] KLab. イージスガード. http://www.klab.jp/ag/aegisguard/. 2012 年 5 月確認.

[76] SignaCert. ホワイトリストソリューション. http://japan.signacert.com/. 2012 年 5 月確認.

[77] 原田季栄, 保理江高志, 田中一男. プロセス実行履歴に基づくアクセスポリシー自動生成システム. *Network Security Forum 2003*.

[78] ジェフラスキン. ヒューメイン・インタフェース - 人に優しいシステムへの新たな指針. ピアソンエデュケーション, Sep. 2001.

[79] Michele C. S. Lange and Kristin M. Nimsger. *Electronic Evidence And Discovery: What Every Lawyer Should Know*. Amer Bar Assn, Sep. 2004.

[80] Microsoft. Information Rights Management. http://www.microsoft.com/japan/office/previous/2003/business/irm/default.mspx. 2012 年 5 月確認.

[81] Adobe. Adobe LiveCycle Rights Management ES3. http://www.adobe.com/jp/products/livecycle/rightsmanagement/. 2012 年 5 月確認.

[82] CodePlex. Word 2007 Redaction Tool. http://redaction.codeplex.com/. 2012 年 5 月確認.

[83] 株式会社富士通研究所. 世界初!紙と電子データの暗号化技術の開発に成功〜高いセキュリティを確保しながら情報共有が可能に〜. http://pr.fujitsu.com/jp/news/2008/06/10.html. 2012 年 5 月確認.

[84] NRI セキュアテクノロジーズ. SecureCube/Labeling. http://www.nri-secure.co.jp/service/cube/labeling.html. 2012 年 5 月確認.

[85] 富士ゼロックス. 紙文書と電子文書を一つのセキュリティ環境下で管理できる初めての技術を開発. http://news.fujixerox.co.jp/news/2008/0512_security/. 2012 年 5 月確認.

[86] 辻井重男, 萩原栄幸, デジタルフォレンジック研究会（編）. デジタル・フォレンジック事典. 日科技連出版社, Dec. 2006.

[87] 日経コンピュータ 2010 年 4 月 28 日号. 重要ファイルだけを「社外秘」に中身に潜むキーワードで判定, pp. 98–101. 2010.

[88] 日経 NETWORK2010 年 6 月号. なぜ今，日本に上陸するのか？ 情報漏えい対策の DLP 製品が続々発売, pp. 16–17. 2010.

[89] 富士経済. e ドキュメント市場マーケティング調査総覧 2008. 富士キメラ総研, Oct. 2008.

[90] 社団法人電子情報技術産業協会（JEITA）. OCR カタログ用語集（第 2 版）. http://home.jeita.or.jp/is/publica/2009/is-09-jyoutan-7.pdf. 2012 年 5 月確認.

[91] 藤井康広, 海老澤竜, 本多義則, 洲崎誠一. マルチベンダ紙文書漏えい対策システムの一提案. 電子情報通信学会技術研究報告. SITE, 技術と社会・倫理, Vol. 108, No. 160, pp. 51–58, 2008.

[92] Microsoft. Windows Driver Kit: Print Devices, Rendering a Print Job. http://preview.library.microsoft.com/en-us/library/ff561943(v=vs.85).aspx. 2012 年 5 月確認.

[93] 奈良先端科学技術大学院大学情報科学研究科自然言語処理学講座（松本研究室）. ChaSen – 形態素解析器. http://chasen-legacy.sourceforge.jp/. 2012 年 5 月確認.

[94] 日本の苗字 7000 傑. http://www.myj7000.jp-biz.net/. 2012 年 5 月確認.

[95] ヤコブニールセン. ユーザビリティエンジニアリング原論 - ユーザーのためのインタフェースデザイン (情報デザインシリーズ). 東京電機大学出版局, 第 2 版, Jul. 2002.

[96] Verizon. Verizon 2011 data breach investigations report. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf. 2012 年 5 月確認.

[97] 京都大学. 環境報告書 2011. http://www.esho.kyoto-u.ac.jp/?p=779. 2012 年 5 月確認.

[98] INAX. コピー用紙の使用量. http://inax.lixil.co.jp/eco/environment_data/detail/copy.html. 2012 年 5 月確認.

[99] Bill Nelson, Frank Enfinger, Ameria Phillips, and Cgris Steuart. コンピュータフォレンジックス入門 - 不正アクセス, 情報漏洩に対する調査と分析 (トムソンセキュリティシリーズ). ビー・エヌ・エヌ新社, Dec. 2005.

[100] 佐々木隆仁. デジタルデータは消えない (幻冬舎ルネッサンス新書 さ 2-1). 幻冬舎ルネッサンス, Mar. 2011.

[101] ケビンマンディア, クリスプロサイス, 坂井順行. インシデントレスポンス - 不正アクセスの発見と対策. 翔泳社, Jul. 2002.

[102] B. Carrier and E.H. Spafford. An event-based digital forensic investigation framework. In *Digital forensic research workshop*, 2004.

[103] S. Ciardhuáin. An extended model of cybercrime investigations. *International Journal of Digital Evidence*, Vol. 3, No. 1, pp. 1–22, 2004.

[104] S.R. Selamat, R. Yusof, and S. Sahib. Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, Vol. 8, No. 10, pp. 163–169, 2008.

[105] K. Kent, S. Chevalier, T. Grance, and H. Dang. Guide to integrating forensic techniques into incident response. *NIST Special Publication 800-86*, 2006.

[106] AccessData. Forensic Toolkit (FTK). http://accessdata.com/products/computer-forensics/ftk. 2012 年 5 月確認.

[107] Guidance Software. EnCase Forensic. http://www.guidancesoftware.com/forensic.htm. 2012年5月確認.

[108] 富士キメラ総研. ネットワークセキュリティビジネス調査総覧 ２０１１上巻（市場編）. 富士キメラ総研, Jul. 2011.

[109] Microsoft. マイクロソフトサーバ製品のログ監査ガイド 印刷ジョブについての監査. http://technet.microsoft.com/ja-jp/solutionaccelerators/dd285678. 2012年5月確認.

[110] Satoshi Kai and Tetsutaro Uehara. Development of a Distributed Print-Out Monitoring System for Efficient Forensic Investigation. In *Proceedings of the Conference on Digital Forensics, Security, and Law 2011*, pp. 109–122, May 2011.

[111] 甲斐賢, 笈川光浩, 伊川宏美, 今一修, 森本康嗣, 土田健一, 手塚悟, 荒井正人, 洲崎誠一. 文字コード処理方式による高速な印刷コントロール機能の開発. 情報処理学会論文誌, Vol. 52, No. 2, pp. 645–655, 2011-02-15.

[112] K. Fujita, Y. Ashino, T. Uehara, and R. Sasaki. Using boot control to preserve the integrity of evidence. *Advances in Digital Forensics IV*, pp. 61–74, 2008.

[113] K. Uematsu and R. Sasaki. A Proposal of Falsification Detection System in Structural Design. In *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on*, pp. 137–142. IEEE, 2008.

[114] A. Yu, Y. Qin, and D. Wang. Obtaining the Integrity of Your Virtual Machine in the Cloud. In *Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on*, pp. 213–222. IEEE, 2011.

[115] Google. Google 検索アプライアンス. http://www.google.com/enterprise/search/. 2012年5月確認.

[116] N2SM, Inc. オープンソース全文検索サーバー fess (フェス). http://fess.sourceforge.jp/ja/. 2012年5月確認.

[117] 小野束, 江川雄毅. 印刷耐性のある電子透かし方式の検討 (セキュリティと社会). 情報処理学会論文誌, Vol. 45, No. 3, pp. 880–890, 2004.

[118] 日立ソリューションズ. 秘文 AE Watermark Print. http://www.hitachi-solutions.co.jp/hibun/sp/product/ae_wmp.html. 2012 年 5 月確認.

[119] 日立 INS ソフトウェア. 電子透かしプリントソリューション. http://www.hitachi-ins.com/products/eshimon/. 2012 年 5 月確認.

[120] Japan Forensic Institute. フォレンジック調査依頼フォーム. https://aos.com/fss/request.html. 2012 年 5 月確認.

[121] AccessData. Processing performance testing and system configuration. http://accessdata.com/downloads/media/FTK_Performance_Testing.pdf. 2012 年 5 月確認.

[122] Microsoft. Windows Driver Kit (WDK) について. http://msdn.microsoft.com/ja-jp/windows/hardware/gg487428. 2012 年 5 月確認.

[123] 社団法人電子情報技術産業協会. JEITA 規格 プリンタ用標準テストパターン（JEITA IT-3011）. JEITA, 2003.

[124] Microsoft. XPS Specification and License Downloads. http://msdn.microsoft.com/en-us/windows/hardware/gg463375.aspx. 2012 年 5 月確認.

[125] 海老澤竜, 藤井康広, 高橋由泰, 手塚悟. 紙文書に対するセキュリティ技術の考察. 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, Vol. 106, No. 176, pp. 75–81, 2006.

[126] Canon. imageWARE Secure Audit Manager. http://cweb.canon.jp/software/output/lineup/secureaudit/. 2012 年 5 月確認.

[127] RICOH. Ridoc IO Data Selector. http://www.ricoh.co.jp/IPSiO/related_goods/dataselector/. 2012 年 5 月確認.

[128] 藤井勇作, 堀田悦伸. A-7-12 EMF 形式印刷データへの文字認識処理による機密文書の検出 (A-7. 情報セキュリティ, 一般セッション). 電子情報通信学会ソサイエティ大会講演論文集, Vol. 2010, p. 124, 2010.

[129] 内田勝也, 高橋正和. 有害プログラム - その分類・メカニズム・対策 (サイバーセキュリティ・シリーズ). 共立出版, Jul. 2004.

[130] 本城信輔. PC のウイルスを根こそぎ削除する方法 - - コンピュータウイルス（マルウェア）は，あなたのお金と情報を狙っている！(Software Design plus). 技術評論社, Oct. 2011.

[131] 独立行政法人 情報処理推進機構セキュリティセンター. コンピュータウイルスによる企業の被害額を 4,400 億円と試算. http://www.ipa.go.jp/security/fy14/reports/current/model-4400.html. 2012 年 5 月確認.

[132] IDC. Business continuity in 2002: It's not business as usual, Apr. 2002.

[133] 独立行政法人 情報処理推進機構セキュリティセンター.「W32/Sircam」に関する情報. http://www.ipa.go.jp/security/topics/sircam.html. 2012 年 5 月確認.

[134] 佐々木慎一, 荒井正人, 永井康彦, 梅都利和. マルチ OS 環境を利用したアクセス制御システムの実装と性能評価. 情報処理学会研究報告. CSEC,[コンピュータセキュリティ], Vol. 2001, No. 75, pp. 157–163, 2001.

[135] 荒井正人, 佐々木慎一, 梅都利和, 永井康彦. マルチ OS 環境を利用したアクセス制御システムの実装と性能評価. 情報処理学会論文誌, Vol. 44, No. 4, pp. 1092–1100, 2003.

[136] 独立行政法人 情報処理推進機構セキュリティセンター. セキュアなインターネットサーバー構築に関する調査（トラステッド OS 利用とセキュア Web プログラミング）. http://www.ipa.go.jp/security/fy14/contents/trusted-os/guide.html. 2012 年 5 月確認.

[137] 中村雄一, 鮫島吉喜. Security-Enhanced Linux のアクセス制御ポリシ設定の簡易化. In *Symposium on Cyrptography and Information Security 2003*, 2003.

[138] 田端利宏, 櫻井幸一. ファイルアクセスパーミッションの統合手法とそのトレードオフに関する考察. 2005 年 暗号と情報セキュリティシンポジウム (SCIS 2005) 予稿集, January, Vol. 1, pp. 79–84, 2005.

[139] 山口拓人, 中村雄一, 田端利宏. ファイルのアクセスベクタパーミッションを統合したアクセスパーミッションの安全性評価. 情報処理学会コンピュータセキュリティシンポジウム 2007 論文集, 2007.

[140] Peter D. Hipson. システム管理者のための Windows2000 Server レジストリガイド. ソフトバンククリエイティブ, Sep. 2000.

[141] 甲斐賢, 荒井正人, 永井康彦, 冨田理. クライアント向けファイルアクセス制御ポリシーの設計と簡易設定方法. 情報処理学会研究報告. CSEC,[コンピュータセキュリティ], Vol. 2003, No. 74, pp. 257–264, 2003.

[142] デイヴィッド・ブルックス. 人生の科学: 「無意識」があなたの一生を決める. 早川書房, Feb. 2012.

[143] NPO 日本ネットワークセキュリティ協会（JNSA）. オフィスの節電対策のための「在宅勤務における情報セキュリティ対策ガイドブック」. http://www.jnsa.org/result/2011/zaitaku_guide.html. 2012 年 6 月確認.

[144] @IT. 「Citrix Synergy 2012」が開幕“ ライフスライス ”によりふさわしいテクノロジを提供する〜シトリックス CEO. http://www.atmarkit.co.jp/news/201205/10/citrix.html. 2012 年 6 月確認.

[145] 経済産業省. 営業秘密 〜営業秘密を守り活用する〜, 営業秘密管理指針. http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html. 2012 年 6 月確認.

[146] 日本スマートフォンセキュリティフォーラム（JSSEC）. スマートフォン&タブレットの業務利用に関するセキュリティガイドライン〜その特性を活かしたワークスタイル変革のために〜 【第一版】. http://www.soumu.go.jp/main_content/000140059.pdf. 2012 年 6 月確認.

[147] 松永英明. 東日本大震災でわたしも考えた. 密林社, Jul. 2011.

主要業績

学術論文誌

1. 甲斐賢, 荒井正人, 永井康彦, 冨田理, 手塚悟. 不正プログラムから情報資産を保護するクライアント向けファイルアクセス制御方式の提案. 情報処理学会論文誌, Vol.46, No.8, pp.1912-1922, Aug. 2005.（5 章に該当）

2. 甲斐賢, 笈川光浩, 伊川宏美, 今一修, 森本康嗣, 土田健一, 手塚悟, 荒井正人, 洲崎誠一. 文字コード処理方式による高速な印刷コントロール機能の開発. 情報処理学会論文誌, Vol.52, No.2, pp.645-655, Nov. 2011.（3 章に該当）

3. 甲斐賢, 上原哲太郎, 喜多一. 効率的なフォレンジック調査のための印刷監視システムの開発. 電子情報通信学会論文誌, Vol.J95-D, No.9, pp.1-11, Sep. 2012.（4 章に該当）

国際学会

1. Satoshi Kai, Tetsutaro Uehara. Development of a Distributed Print-Out Monitoring System for Efficient Forensic Investigation. In Proceedings of the Conference on Digital Forensics, Security, and Law 2011, pp.109-122, May 2011.（4 章に該当）

特許

1. 荒井 正人, 甲斐 賢. ポリシー設定支援ツール. 特開 2004-192601. Jul. 2004.（5 章に該当）

2. 甲斐 賢, 荒井 正人, 土田 健一. 印刷物管理システム. 特開 2010-015538. Jan. 2010.（3 章に該当）

登録商標の表記

Windows，Windows 2000, Windows XP は，米国 Microsoft Corporation の米国およびその他の国における登録商標です.

Microsoft Word，Microsoft Excel は，米国 Microsoft Corporation の商品名称です．Microsoft PowerPoint は，米国 Microsoft Corporation の米国およびその他の国における商標です.

OLE は，Microsoft Corporation が開発したソフトウェア名称です．OLE は，Object Linking and Embedding の略です.

Acrobat，Acrobat Reader, PDF は，Adobe Systems Incorporated の米国およびその他の国における登録商標です.

VMware は，VMware, Inc. の米国およびその他の国での商標または登録商標です.

Intel Core 2 Duo は，Intel Corporation の米国およびその他の国における登録商標です.

Linux の名称は，Linus Torvalds の米国およびその他の国における登録商標あるいは商標です.

Citrix は，Citrix Systems, Inc の米国およびその他の国における商標または登録商標です.

その他文中の社名，商品名は，各社の商標または登録商標です.